GS2200-8/24 Series

Intelligent Layer 2 GbE Switch

User's Guide

Default Login Details

IP Address	http://192.168.1.1
User Name	admin
Password	1234

Firmware Version 4.00
Edition 1, 12/2011

ZyXEL

www.zyxel.com

Copyright © 2011
ZyXEL Communications Corporation

About This User's Guide

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Intended Audience

This manual is intended for people who want to configure the Switch using the web configurator.

Related Documentation

- Command Line Interface (CLI) Reference Guide

  The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the Switch.

- Web Configurator Online Help

  The embedded Web Help contains descriptions of individual screens and supplementary information.

Note: It is recommended you use the web configurator to configure the Switch.

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.

- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.

- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

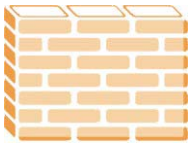
Syntax Conventions

- The GS2200-8, GS2200-8HP, GS2200-24 and GS2200-24P may be referred to as the "Switch", the "device", the "system" or the "product" in this User's Guide. Differentiation is made where needed.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

The Switch	Computer	Notebook computer

Server	DSLAM	Firewall 
Telephone	Router	

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Do not obstruct the device ventillation slots as insufficient airflow may harm your device.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Use ONLY power wires of the appropriate wire gauge (see Chapter 43 on page 307 for details) for your device. Connect it to a power supply of the correct voltage (see Chapter 43 on page 307 for details).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

User's Guide 21

Getting to Know Your Switch 23
Hardware Installation and Connection 27
Hardware Panels 31

Technical Reference 37

The Web Configurator 39
Initial Setup Example 47
Tutorials 51
System Status and Port Statistics 60
Basic Setting 66
VLAN 83
Static MAC Forward Setup 101
Static Multicast Forward Setup 103
Filtering 107
Spanning Tree Protocol 109
Bandwidth Control 129
Broadcast Storm Control 132
Mirroring 134
Link Aggregation 137
Port Authentication 145
Port Security 151
Classifier 154
Policy Rule 160
Queuing Method 165
Multicast 168
AAA 182
IP Source Guard 193
Loop Guard 215
Layer 2 Protocol Tunneling 219
PPPoE 223
Error Disable 231
Static Route 237
Differentiated Services 240
DHCP 244
ARP Learning 250
Maintenance 255
Access Control 261

Diagnostic 285
Syslog 287
Cluster Management 290
MAC Table 296
ARP Table 299
Configure Clone 301
Troubleshooting 303
Product Specifications 307

Table of Contents

About This User's Guide 3

Document Conventions 6

Safety Warnings 8

Contents Overview 9

Table of Contents 11

Part I: User's Guide 21

Chapter 1
Getting to Know Your Switch 23

1.1 Introduction 23
1.1.1 Backbone Application 23
1.1.2 Bridging Example 24
1.1.3 High Performance Switching Example 24
1.1.4 IEEE 802.1Q VLAN Application Examples 25
1.2 Ways to Manage the Switch 26
1.3 Good Habits for Managing the Switch 26

Chapter 2
Hardware Installation and Connection 27

2.1 Installation Scenarios 27
2.2 Desktop Installation Procedure 27
2.3 Mounting the Switch on a Rack 27
2.3.1 Rack-mounted Installation Requirements 27
2.3.2 Attaching the Mounting Brackets to the Switch 28
2.3.3 Mounting the Switch on a Rack 29
2.4 Wall Mounting (for GS2200-8 only) 29

Chapter 3
Hardware Panels 31

3.1 Overview 31
3.2 Front Panels 31
3.2.1 Console Port 33
3.2.2 Gigabit Ethernet Ports 33
3.2.3 Mini-GBIC Slots 34

3.2.4 Power Connector 35
3.3 LEDs 36

Part II: Technical Reference 37

Chapter 4
The Web Configurator 39

4.1 Overview 39
4.2 System Login 39
4.3 The Status Screen 40
4.3.1 Change Your Password 44
4.4 Saving Your Configuration 44
4.5 Switch Lockout 44
4.6 Resetting the Switch 45
4.6.1 Reload the Configuration File 45
4.7 Logging Out of the Web Configurator 46
4.8 Help 46

Chapter 5
Initial Setup Example 47

5.1 Overview 47
5.1.1 Creating a VLAN 47
5.1.2 Setting Port VID 48
5.2 Configuring Switch Management IP Address 49

Chapter 6
Tutorials 51

6.1 Overview 51
6.2 How to Use DHCP Snooping on the Switch 51
6.3 How to Use DHCP Relay on the Switch 54
6.3.1 DHCP Relay Tutorial Introduction 55
6.3.2 Creating a VLAN 55
6.3.3 Configuring DHCP Relay 58
6.3.4 Troubleshooting 59

Chapter 7
System Status and Port Statistics 60

7.1 Overview 60
7.1.1 What You Can Do 60
7.2 Port Status Summary 61
7.2.1 Status: Port Details 63

Chapter 8
Basic Setting 66

8.1 Overview 66
8.1.1 What You Can Do 66
8.2 System Information 67
8.3 General Setup 69
8.4 Introduction to VLANs 70
8.5 Switch Setup Screen 71
8.6 IP Setup 72
8.6.1 Management IP Addresses 73
8.7 Port Setup 75
8.8 PoE Status 76
8.8.1 PoE Setup 79

Chapter 9
VLAN 83

9.1 Overview 83
9.1.1 What You Can Do 83
9.1.2 What You Need to Know 83
9.2 VLAN Status 86
9.2.1 VLAN Details 87
9.3 Configure a Static VLAN 88
9.4 Configure VLAN Port Settings 90
9.5 Subnet Based VLANs 91
9.5.1 Configuring Subnet Based VLAN 92
9.6 Protocol Based VLANs 94
9.6.1 Configuring Protocol Based VLAN 94
9.7 Port-based VLAN Setup 96
9.7.1 Configure a Port-based VLAN 97
9.8 Technical Reference 99
9.8.1 Create an IP-based VLAN Example 99

Chapter 10
Static MAC Forward Setup 101

10.1 Overview 101
10.1.1 What You Can Do 101
10.2 Configuring Static MAC Forwarding 101

Chapter 11
Static Multicast Forward Setup 103

11.1 Overview 103
11.1.1 What You Can Do 103
11.1.2 What You Need To Know 103

11.2 Configuring Static Multicast Forwarding 104

Chapter 12
Filtering 107

12.1 Overview 107
12.1.1 What You Can Do 107
12.2 Configure a Filtering Rule 107

Chapter 13
Spanning Tree Protocol 109

13.1 Overview 109
13.1.1 What You Can Do 109
13.1.2 What You Need to Know 109
13.2 Spanning Tree Protocol Status Screen 112
13.3 Spanning Tree Configuration 113
13.4 Configure Rapid Spanning Tree Protocol 114
13.5 Rapid Spanning Tree Protocol Status 115
13.6 Configure Multiple Rapid Spanning Tree Protocol 117
13.7 Multiple Rapid Spanning Tree Protocol Status 118
13.8 Configure Multiple Spanning Tree Protocol 120
13.8.1 Multiple Spanning Tree Protocol Port Configuration 123
13.9 Multiple Spanning Tree Protocol Status 123
13.10 Technical Reference 125
13.10.1 MSTP Network Example 126
13.10.2 MST Region 126
13.10.3 MST Instance 127
13.10.4 Common and Internal Spanning Tree (CIST) 127

Chapter 14
Bandwidth Control 129

14.1 Overview 129
14.1.1 What You Can Do 129
14.2 Bandwidth Control Setup 130

Chapter 15
Broadcast Storm Control 132

15.1 Overview 132
15.1.1 What You Can Do 132
15.2 Broadcast Storm Control Setup 133

Chapter 16
Mirroring 134

16.1 Overview 134

16.1.1 What You Can Do 134
16.2 Port Mirroring Setup 135

Chapter 17
Link Aggregation 137

17.1 Overview 137
17.1.1 What You Can Do 137
17.1.2 What You Need to Know 137
17.2 Link Aggregation Status 138
17.3 Link Aggregation Setting 140
17.4 Link Aggregation Control Protocol 142
17.5 Technical Reference 143
17.5.1 Static Trunking Example 143

Chapter 18
Port Authentication 145

18.1 Overview 145
18.1.1 What You Can Do 145
18.1.2 What You Need to Know 145
18.2 Port Authentication Configuration 146
18.3 Activate IEEE 802.1x Security 147
18.3.1 Guest VLAN 148

Chapter 19
Port Security 151

19.1 Overview 151
19.1.1 What You Can Do 151
19.2 Port Security Setup 152

Chapter 20
Classifier 154

20.1 Overview 154
20.1.1 What You Can Do 154
20.1.2 What You Need to Know 154
20.2 Configuring the Classifier 154
20.2.1 Viewing and Editing Classifier Configuration 156
20.3 Classifier Example 158

Chapter 21
Policy Rule 160

21.1 Policy Rules Overview 160
21.1.1 What You Can Do 160
21.2 Configuring Policy Rules 160

21.2.1 Viewing and Editing Policy Configuration 163
21.3 Policy Example 164

Chapter 22
Queuing Method 165

22.1 Overview 165
22.1.1 What You Can Do 165
22.1.2 What You Need to Know 165
22.2 Configuring Queuing 166

Chapter 23
Multicast 168

23.1 Overview 168
23.1.1 What You Can Do 168
23.1.2 What You Need to Know 168
23.2 Multicast Status 170
23.3 Multicast Setting 171
23.4 IGMP Snooping VLAN 174
23.5 IGMP Filtering Profile 175
23.6 The MVR Screen 176
23.6.1 MVR Group Configuration 178
23.6.2 MVR Configuration Example 179

Chapter 24
AAA 182

24.1 Overview 182
24.1.1 What You Can Do 182
24.1.2 What You Need to Know 182
24.2 AAA Screens 183
24.3 RADIUS Server Setup 183
24.4 TACACS+ Server Setup 186
24.5 AAA Setup 188
24.6 Technical Reference 190
24.6.1 Vendor Specific Attribute 190
24.6.2 Supported RADIUS Attributes 191
24.6.3 Attributes Used for Authentication 192

Chapter 25
IP Source Guard 193

25.1 Overview 193
25.1.1 What You Can Do 193
25.1.2 What You Need to Know 194
25.2 IP Source Guard 194

25.3 IP Source Guard Static Binding 195
25.4 DHCP Snooping 196
25.5 DHCP Snooping Configure 199
25.5.1 DHCP Snooping Port Configure 201
25.5.2 DHCP Snooping VLAN Configure 203
25.6 ARP Inspection Status 204
25.7 ARP Inspection VLAN Status 205
25.8 ARP Inspection Log Status 206
25.9 ARP Inspection Configure 207
25.9.1 ARP Inspection Port Configure 208
25.9.2 ARP Inspection VLAN Configure 210
25.10 Technical Reference 211
25.10.1 DHCP Snooping Overview 211
25.10.2 ARP Inspection Overview 213

Chapter 26
Loop Guard 215

26.1 Overview 215
26.1.1 What You Can Do 215
26.1.2 What You Need to Know 215
26.2 Loop Guard Setup 217

Chapter 27
Layer 2 Protocol Tunneling 219

27.1 Overview 219
27.1.1 What You Can Do 219
27.1.2 What You Need to Know 219
27.2 Configuring Layer 2 Protocol Tunneling 221

Chapter 28
PPPoE 223

28.1 PPPoE Intermediate Agent Overview 223
28.1.1 What You Can Do 223
28.1.2 What You Need to Know 223
28.2 The PPPoE Screen 225
28.3 PPPoE Intermediate Agent 226
28.3.1 PPPoE IA Per-Port 227
28.3.2 PPPoE IA Per-Port Per-VLAN 228
28.3.3 PPPoE IA for VLAN 230

Chapter 29
Error Disable 231

29.1 Overview 231

29.1.1 What You Can Do 231
29.1.2 What You Need to Know 231
29.2 The Error Disable Screen 232
29.3 CPU Protection Configuration 232
29.4 Error-Disable Detect Configuration 233
29.5 Error-Disable Recovery Configuration 234

Chapter 30
Static Route 237

30.1 Overview 237
30.1.1 What You Can Do 237
30.2 Configuring Static Routing 238

Chapter 31
Differentiated Services 240

31.1 Overview 240
31.1.1 What You Can Do 240
31.1.2 What You Need to Know 240
31.2 Activating DiffServ 241
31.3 DSCP-to-IEEE 802.1p Priority Settings 242
31.3.1 Configuring DSCP Settings 242

Chapter 32
DHCP 244

32.1 DHCP Overview 244
32.1.1 What You Can Do 244
32.1.2 What You Need to Know 244
32.2 DHCP Status 245
32.3 Configuring DHCP Global Relay 246
32.3.1 Global DHCP Relay Configuration Example 247
32.4 Configuring DHCP VLAN Settings 247
32.4.1 Example: DHCP Relay for Two VLANs 248

Chapter 33
ARP Learning 250

33.1 ARP Overview 250
33.1.1 What You Can Do 250
33.1.2 What You Need to Know 250
33.2 Configuring ARP Learning 252

Chapter 34
Maintenance 255

34.1 Overview 255

34.1.1 What You Can Do 255
34.2 The Maintenance Screen 255
34.2.1 Load Factory Default 256
34.2.2 Save Configuration 256
34.2.3 Reboot System 257
34.3 Firmware Upgrade 257
34.4 Restore a Configuration File 258
34.5 Backup a Configuration File 258
34.6 Technical Reference 259
34.6.1 FTP Command Line 259
34.6.2 Filename Conventions 259
34.6.3 FTP Command Line Procedure 259
34.6.4 GUI-based FTP Clients 260
34.6.5 FTP Restrictions 260

Chapter 35
Access Control 261

35.1 Overview 261
35.1.1 What You Can Do 261
35.2 The Access Control Main Screen 261
35.3 Configuring SNMP 262
35.3.1 Configuring SNMP Trap Group 264
35.3.2 Configuring SNMP User 265
35.4 Setting Up Login Accounts 266
35.5 Service Port Access Control 268
35.6 Remote Management 268
35.7 Technical Reference 270
35.7.1 About SNMP 270
35.7.2 SSH Overview 277
35.7.3 Introduction to HTTPS 278

Chapter 36
Diagnostic 285

36.1 Overview 285
36.2 Diagnostic 285

Chapter 37
Syslog 287

37.1 Overview 287
37.1.1 What You Can Do 287
37.2 Syslog Setup 287
37.3 Syslog Server Setup 289

Chapter 38
Cluster Management 290

38.1 Overview 290
38.1.1 What You Can Do 291
38.2 Cluster Management Status 291
38.3 Clustering Management Configuration 292
38.4 Technical Reference 294
38.4.1 Cluster Member Switch Management 294

Chapter 39
MAC Table 296

39.1 Overview 296
39.1.1 What You Can Do 296
39.1.2 What You Need to Know 296
39.2 Viewing the MAC Table 297

Chapter 40
ARP Table 299

40.1 Overview 299
40.1.1 What You Can Do 299
40.1.2 What You Need to Know 299
40.2 Viewing the ARP Table 299

Chapter 41
Configure Clone 301

41.1 Overview 301
41.2 Configure Clone 301

Chapter 42
Troubleshooting 303

42.1 Power, Hardware Connections, and LEDs 303
42.2 Switch Access and Login 304
42.3 Switch Configuration 306

Chapter 43
Product Specifications 307

Appendix A Changing a Fuse 315

Appendix B Common Services 317

Appendix C Legal Information 321

Index 323

PART I
User's Guide

1

Getting to Know Your Switch

1.1 Introduction

This chapter introduces the main features and applications of the Switch.

The Switch is a layer-2 standalone Ethernet switch with additional layer-2, layer-3, and layer-4 features suitable for Ethernets. The Switch has eight or twenty-four 100/1000 Mbps Ethernet ports. It also has two or four GbE dual personality interfaces with each interface comprising one mini-GBIC slot and one 100/1000 Mbps RJ-45 port, with either port or slot active at a time.

With its built-in web configurator, managing and configuring the Switch is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

The G2200-24P and G2200-8HP come with a Power-over-Ethernet (PoE) feature. The GS2200-8HP supports the IEEE 802.3at High Power over Ethernet (PoE) standard and the GS2200-24P supports the IEEE 802.3af PoE standard. Ports 1 to 4 on the GS2200-8HP can supply power of up to 30W per Ethernet port. Ports 5 to 8 on the GS2200-8HP and ports 1 to 24 on the GS2200-24P can supply power of up to 15.4W per Ethernet port.

Key feature differences between Switch models are as follows. Other features are common to all models. See Chapter 43 on page 307 for a full list of software features available on the Switch.

Table 1 Model-Specific Features

FEATURE	SWITCH MODEL
IEEE 802.3af PoE	GS2200-24P
IEEE 802.3at High Power over Ethernet (PoE)	GS2200-8HP
Power management mode - Classification	GS2200-24P
Power management mode - Consumption	GS-2200-8HP, GS2200-24P
Rack mounting	GS2200-8, GS2200-8HP, GS2200-24, GS2200-24P
Wall mounting	GS2200-8

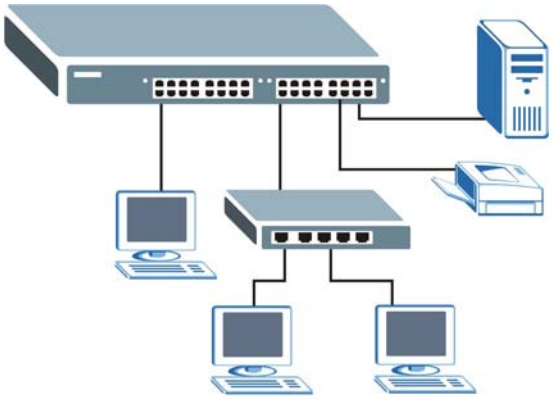
This section shows a few examples of using the Switch in various network environments.

1.1.1 Backbone Application

The Switch is an ideal solution for small networks where rapid growth can be expected in the near future. The Switch can be used standalone for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch.

In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

Figure 1 Backbone Application

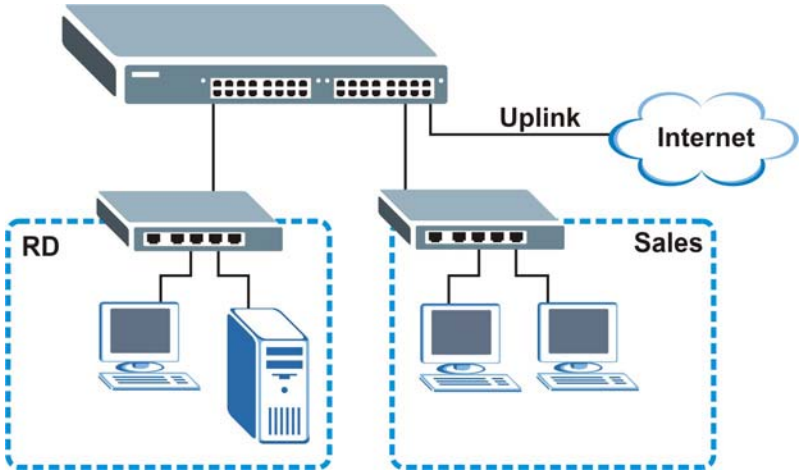


1.1.2 Bridging Example

In this example, the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a super-fast uplink connection by using a Gigabit Ethernet/mini-GBIC port on the Switch.

Moreover, the Switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 2 Bridging Application

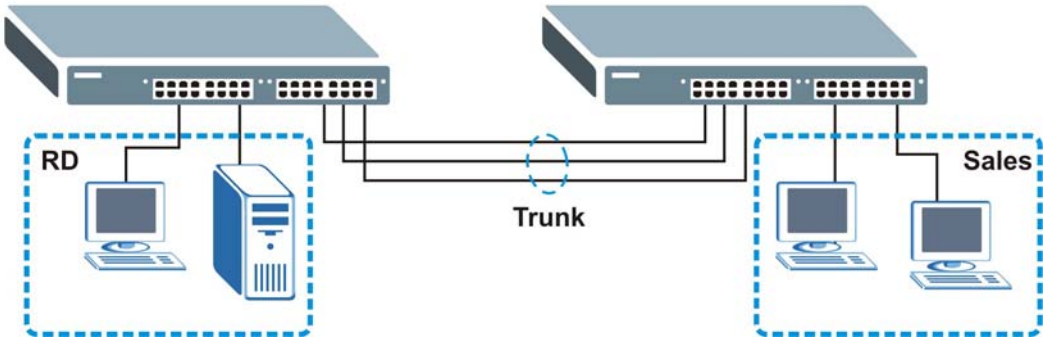


1.1.3 High Performance Switching Example

The Switch is ideal for connecting two networks that need high bandwidth. In the following example, use trunking to connect these two networks.

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The Switch can provide the same bandwidth as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

Figure 3 High Performance Switched Workgroup Application



1.1.4 IEEE 802.1Q VLAN Application Examples

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

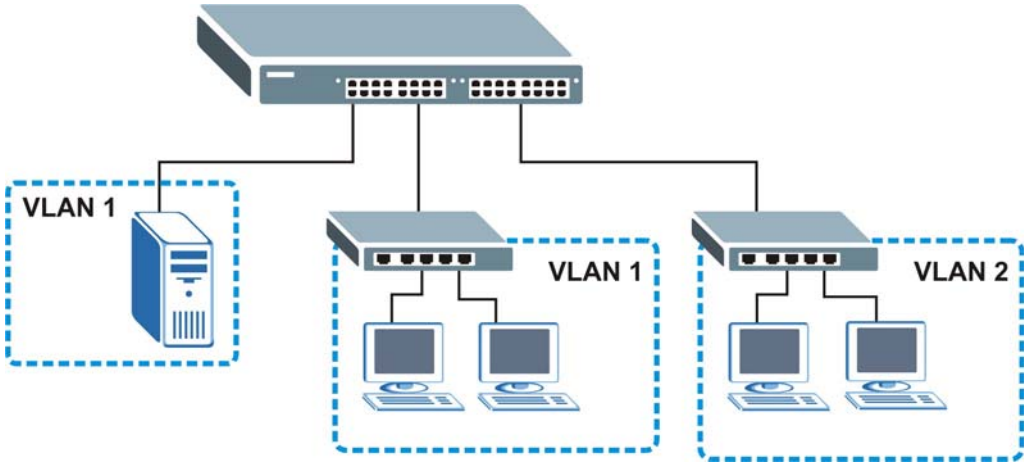
For more information on VLANs, refer to Chapter 9 on page 83.

1.1.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



1.2 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 39.
- Command Line Interface. Line commands offer an alternative to the web configurator and in some cases are necessary to configure advanced features. See the CLI Reference Guide.
- FTP. Use FTP for firmware upgrades and configuration backup/restore. See Section 34.6.1 on page 259.
- SNMP. The Switch can be monitored by an SNMP manager. See Section 35.7.1 on page 270.
- Cluster Management. Cluster Management allows you to manage multiple switches through one switch, called the cluster manager. See Chapter 38 on page 290.

1.3 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration.

2

Hardware Installation and Connection

2.1 Installation Scenarios

This chapter shows you how to install and connect the Switch.

The Switch can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

Note: For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the Switch. This is especially important for enclosed rack installations.

2.2 Desktop Installation Procedure

1 Make sure the Switch is clean and dry.

2 Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.

3 Make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord.

2.3 Mounting the Switch on a Rack

The Switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your Switch on a standard EIA rack using a rack-mounting kit.

2.3.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

Failure to use the proper screws may damage the unit.

2.3.1.1 Precautions

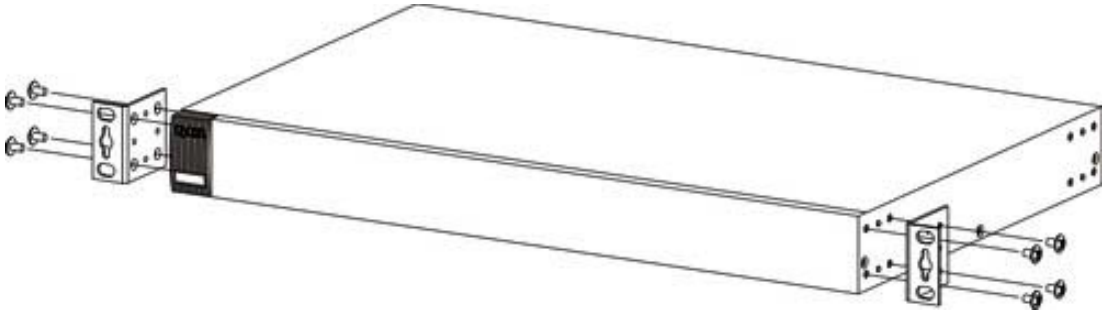
- Make sure the rack will safely support the combined weight of all the equipment it contains.

- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.3.2 Attaching the Mounting Brackets to the Switch

1 Position a mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.

Figure 5 Attaching the Mounting Brackets



2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.

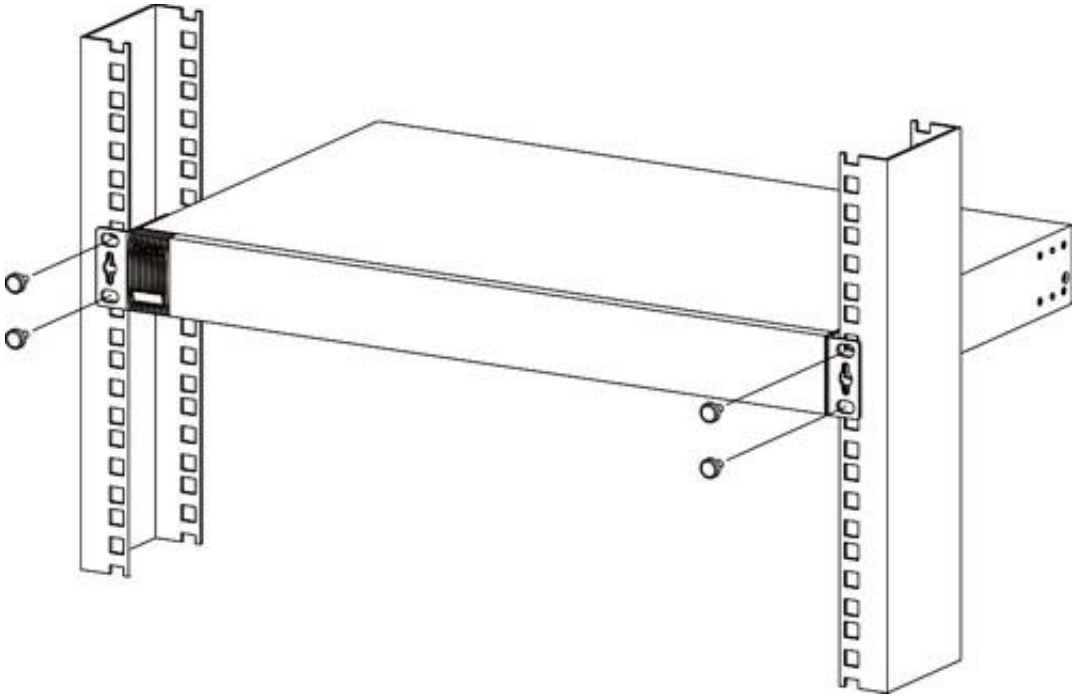
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

4 You may now mount the Switch on a rack. Proceed to the next section.

2.3.3 Mounting the Switch on a Rack

1 Position a mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 6 Mounting the Switch on a Rack



2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

2.4 Wall Mounting (for GS2200-8 only)

Do the following to attach your Switch to a wall.

Insecure mounting may damage the device or cause injury. ZyXEL is not responsible for damages incurred by insecure wall-mounting.

1 Screw the two screws provided with your Switch into the wall 135 mm apart (see Figure 7 on page 30). See Figure 8 on page 30 for the size of screws to use.

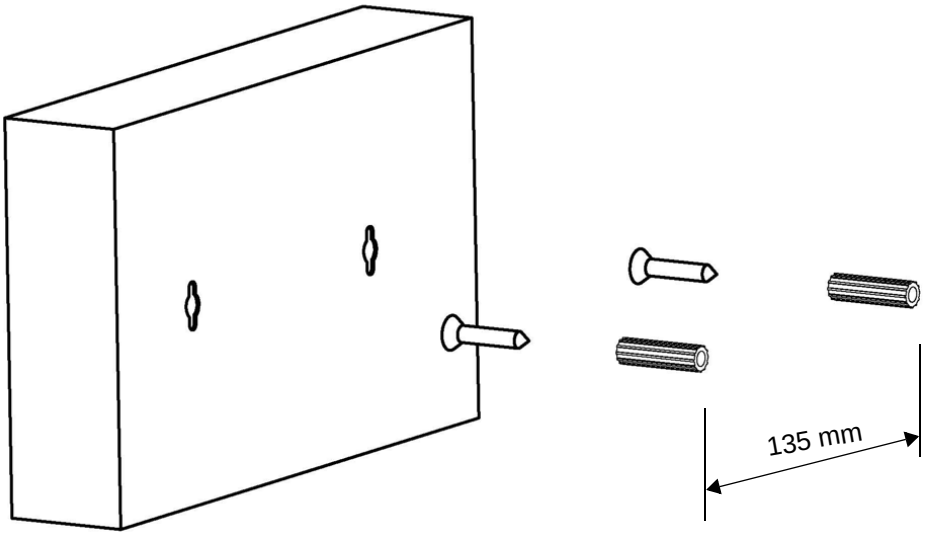
Do not screw the screws all the way in to the wall; leave a small gap between the head of the screw and the wall.

The gap must be big enough for the screw heads to slide into the screw slots and the connection cables to run down the back of the Switch.

Note: Make sure the screws are securely fixed to the wall and strong enough to hold the weight of the Switch with the connection cables.

2 Align the holes on the back of the Switch with the screws on the wall. Hang the Switch on the screws.

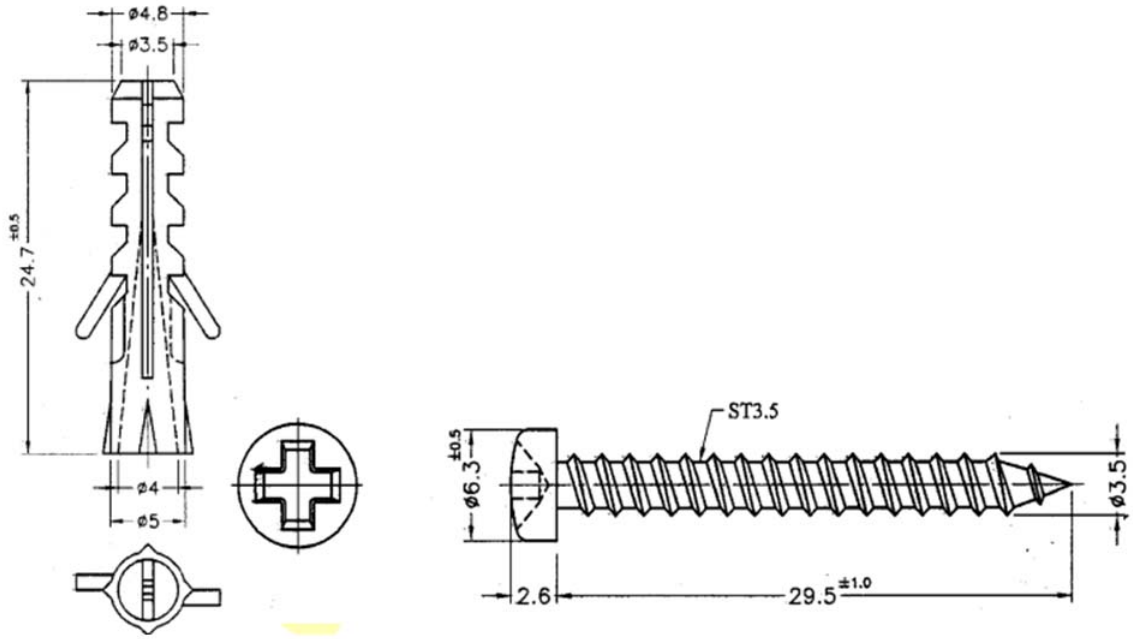
Figure 7 Wall-mounting Example



The Switch should be wall-mounted horizontally. The Switch's side panels with ventilation slots should not be facing up or down as this position is less safe.

The following are dimensions of a self-tapping screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 8 Masonry Plug and 3.5 mm Self-Tapping Screw



3

Hardware Panels

3.1 Overview

This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

3.2 Front Panels

The following figure shows the front panel of the Switch.

Figure 9 Front Panel (GS2200-8)

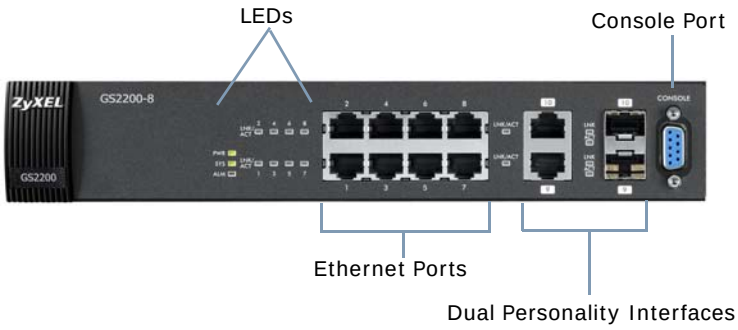


Figure 10 Front Panel (GS2200-8HP)

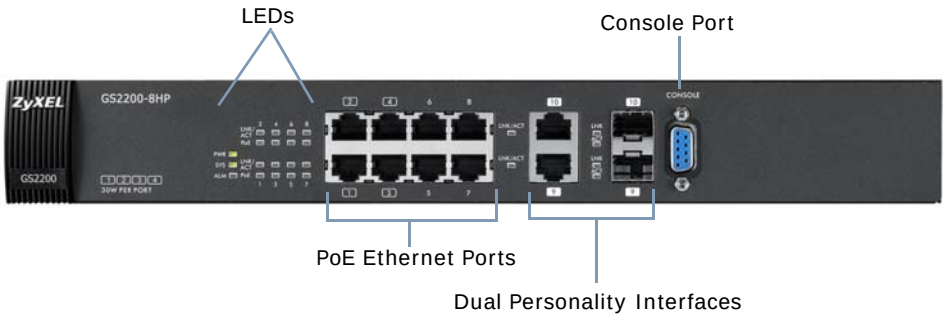


Figure 11 Front Panel (GS2200-24)

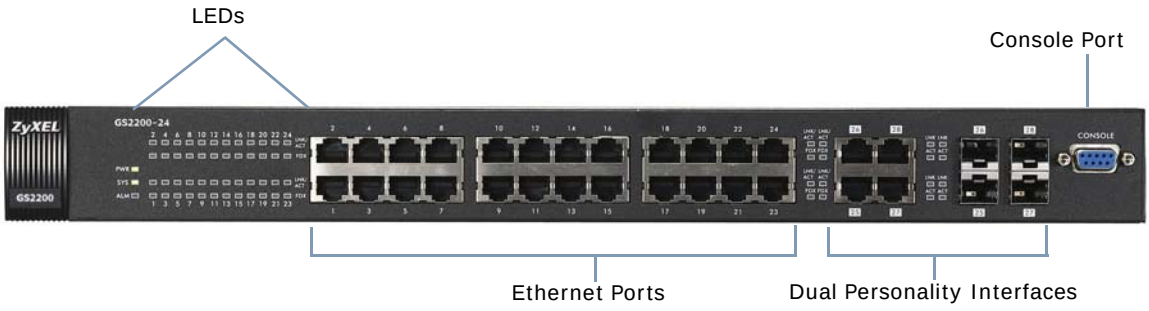
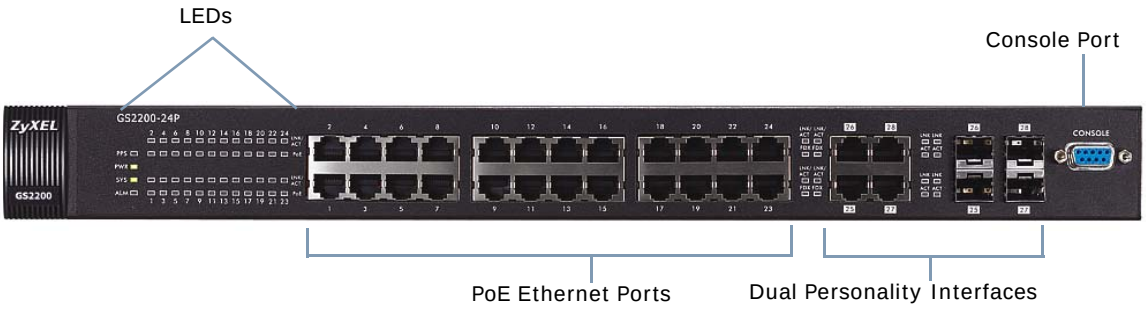


Figure 12 Front Panel (GS2200-24P)



The following table describes the port labels on the front panel.

Table 2 Front Panel Connections

LABEL	DESCRIPTION
8 or 24 100/1000 RJ-45 Ethernet Ports (GS2200-8 or GS2200-24 only)	Connect these ports to a computer, a hub, a wireless AP, an Ethernet switch or router.
8 or 24 100/1000 BASE-T PoE Ports (GS2200-8HP or GS2200-24P only)	Connect these ports to a computer, a hub, a wireless AP, an Ethernet switch or router. The GS2200-8HP supports the IEEE 802.3at High Power over Ethernet (PoE) standard and the GS2200-24P supports the IEEE 802.3af PoE standard. Ports 1 to 4 on the GS2200-8HP can supply power of up to 30W per Ethernet port. Ports 5 to 8 on the GS2200-8HP and ports 1 to 24 on the GS2200-24P can supply power of up to 15.4W per Ethernet port.

Table 2 Front Panel Connections (continued)

LABEL	DESCRIPTION
2 or 4 Dual Personality Interfaces	Each interface has one 100/1000 Mbps RJ-45 port and one Small Form-Factor Pluggable (SFP) slot (also called a mini-GBIC slot), with one port or transceiver active at a time. Note: The ports change to fiber mode directly when inserting the fiber module.
	• Two or four 100/1000 Mbps RJ-45 Ports: Connect these ports to high-bandwidth backbone network Ethernet switches using 1000Base-T compatible Category 5/5e/6 copper cables.
	• Two or four Mini-GBIC Slots: Use mini-GBIC transceivers in these slots for connections to backbone Ethernet switches.
Console Port	The console port is for local configuration of the Switch.

3.2.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100
- Terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.2.2 Gigabit Ethernet Ports

The Switch has 1000Base-T auto-negotiating, auto-crossover Ethernet ports. In 100/1000 Mbps Gigabit Ethernet, the speed can be 100 Mbps or 1000 Mbps and the duplex mode can be half duplex or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

Four 1000Base-T Ethernet ports are paired with a mini-GBIC slot to create a dual personality interface. The Switch uses up to one connection for each mini-GBIC and 1000Base-T Ethernet pair. The mini-GBIC slots have priority over the Gigabit ports. This means that if a mini-GBIC slot and the corresponding GbE port are connected at the same time, the GbE port will be disabled.

Note: The dual personality ports change to fiber mode directly when inserting the fiber module.

When auto-negotiation is turned on, an Ethernet port negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the

signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

3.2.2.1 Default Ethernet Negotiation Settings

The factory default negotiation settings for the Gigabit ports on the Switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Link Aggregation: Disabled

3.2.2.2 Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Gigabit port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

3.2.3 Mini-GBIC Slots

These are slots for mini-GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic or even copper cable connectors.

To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

- Type: SFP connection interface
- Connection speed:

  GS2200-8/8HP: 100 Megabit per second (Mbps) or 1 Gigabit per second (Gbps)

  GS2200-24/24P: 1 Gigabit per second (Gbps)

3.2.3.1 Transceiver Installation

Use the following steps to install a mini-GBIC transceiver (SFP module).

1. Insert the transceiver into the slot with the exposed section of PCB board facing down.
2. Press the transceiver firmly until it clicks into place.
3. The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.
4. Close the transceiver's latch (latch styles vary).

5 Connect the fiber optic cables to the transceiver.

Figure 13 Transceiver Installation Example

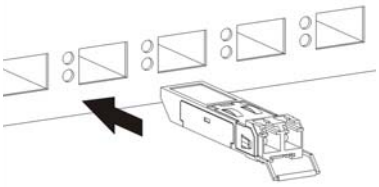
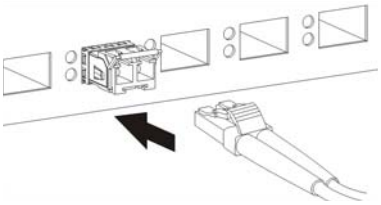


Figure 14 Connecting the Fiber Optic Cables



3.2.3.2 Transceiver Removal

Use the following steps to remove a mini-GBIC transceiver (SFP module).

1 Remove the fiber optic cables from the transceiver.

2 Open the transceiver's latch (latch styles vary).

3 Pull the transceiver out of the slot.

Figure 15 Removing the Fiber Optic Cables

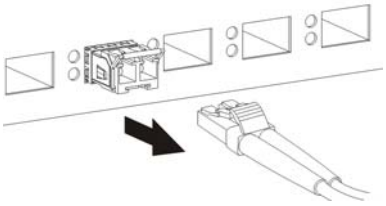


Figure 16 Opening the Transceiver's Latch Example

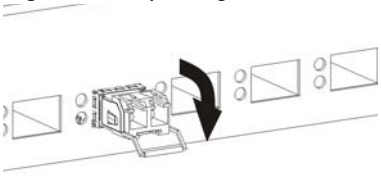
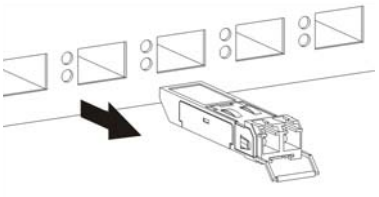


Figure 17 Transceiver Removal Example



3.2.4 Power Connector

Note: Make sure you are using the correct power source as shown on the panel.

To connect power to the Switch, insert the female end of the power cord to the AC power receptacle on the front panel. Connect the other end of the supplied power cord to a power outlet. Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

See Chapter 43 on page 307 for information on the Switch's power supply requirements.

3.3 LEDs

After you connect the power to the Switch, view the LEDs to ensure proper functioning of the Switch and as an aid in troubleshooting.

Table 3 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The system is turned on.
		Off	The system is off or has failed.
SYS	Green	On	The system is on and functioning properly.
		Blinking	The system is rebooting and performing self-diagnostic tests.
		Off	The power is off or the system is not ready/malfunctioning.
PPS (GS2200-24P only)	Green	On	External power supply is turned on.
		Off	External power supply is turned off or has failed.
ALM	Red	On	A hardware failure is detected.
		Off	The system is functioning normally.
Ethernet Ports			
LNK/ACT	Green	Blinking	The system is transmitting/receiving to/from a 1000 Mbps Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
PoE (GS2200-8HP or GS2200-24P only)	Amber	On	Power is supplied to all PoE Ethernet ports.
		Off	There is no power supply.
FDX (GS2200-24 or GS2200-24P only)	Amber	On	The Gigabit port is negotiating in full-duplex mode.
		Off	The Gigabit port is negotiating in half-duplex mode.
Mini-GBIC Slots			
LNK	Green	On	The link to a 1000 Mbps Ethernet network is up.
	Amber (GS2200-8/8HP only)	On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to this port is not connected.
ACT	Green	Blinking	This port is receiving or transmitting data.

PART II
Technical Reference

4

The Web Configurator

4.1 Overview

This section introduces the configuration and functions of the web configurator.

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use Internet Explorer 6.0 and later, Netscape Navigator 7.0 and later, Mozilla Firefox 3.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

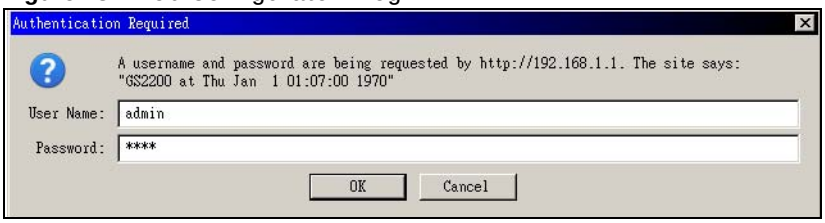
4.2 System Login

1 Start your web browser.

2 Type “http://” and the IP address of the Switch (for example, the default management IP address is 192.168.1.1) in the **Location** or **Address** field. Press [ENTER].

3 The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 18 Web Configurator: Login



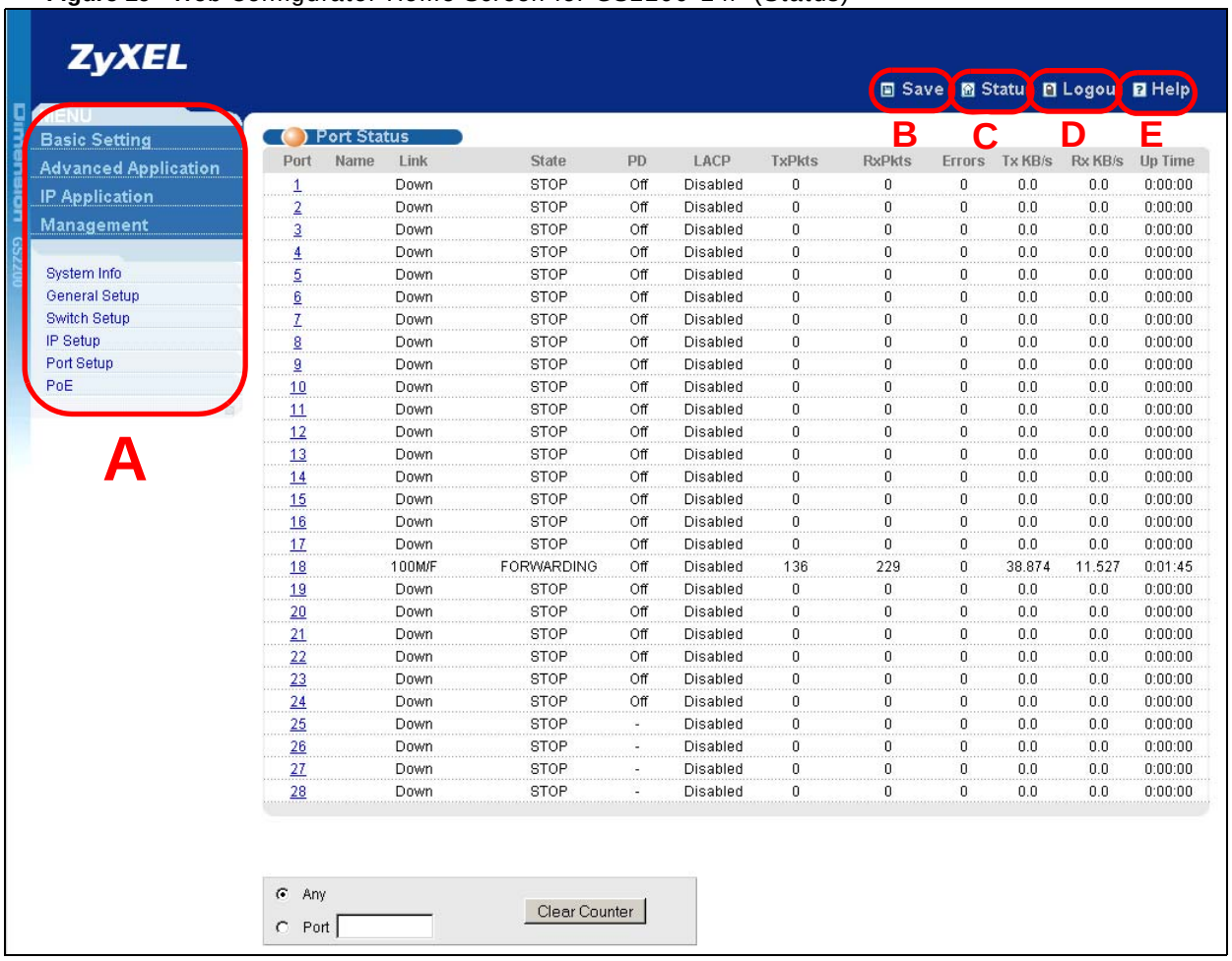
4 Click **OK** to view the first web configurator screen.

4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator. This guide uses the GS2200-24P screens as an example. The screens may vary slightly for different models.

The following figure shows the navigating components of a web configurator screen.

Figure 19 Web Configurator Home Screen for GS2200-24P (Status)



A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

B, **C**, **D**, **E** - These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.

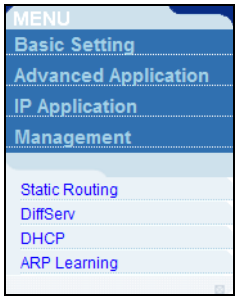
C - Click this link to go to the status page of the Switch.

D - Click this link to logout of the web configurator.

E - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 4 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
GS2200-8/24 **GS2200-8HP/24P** 			

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up to 64 IP routing domains.
Port Setup	This link takes you to a screen where you can configure settings for individual Switch ports.
PoE	(For GS2200-8HP or GS2200-24P only) This link takes you to a screen where you can set priorities so that the Switch is able to reserve and allocate power to certain PDs.
Advanced Application	

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to a screen where you can configure bandwidth limits on the Switch.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication for clients communicating via the Switch.
Port Security	This link takes you to screens where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
Multicast	This link takes you to screens where you can configure various multicast features, IGMP snooping and create multicast VLANs.
AAA	This link takes you to a screen where you can configure authentication, authorization services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
Layer 2 Protocol Tunneling	This link takes you to a screen where you can configure L2PT (Layer 2 Protocol Tunneling) settings on the Switch.
PPPoE	This link takes you to screens where you can configure how the Switch gives a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.
Errdisable	This link takes you to a screen where you can configure CPU protection and error disable recovery.
IP Application	
Static Routing	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.

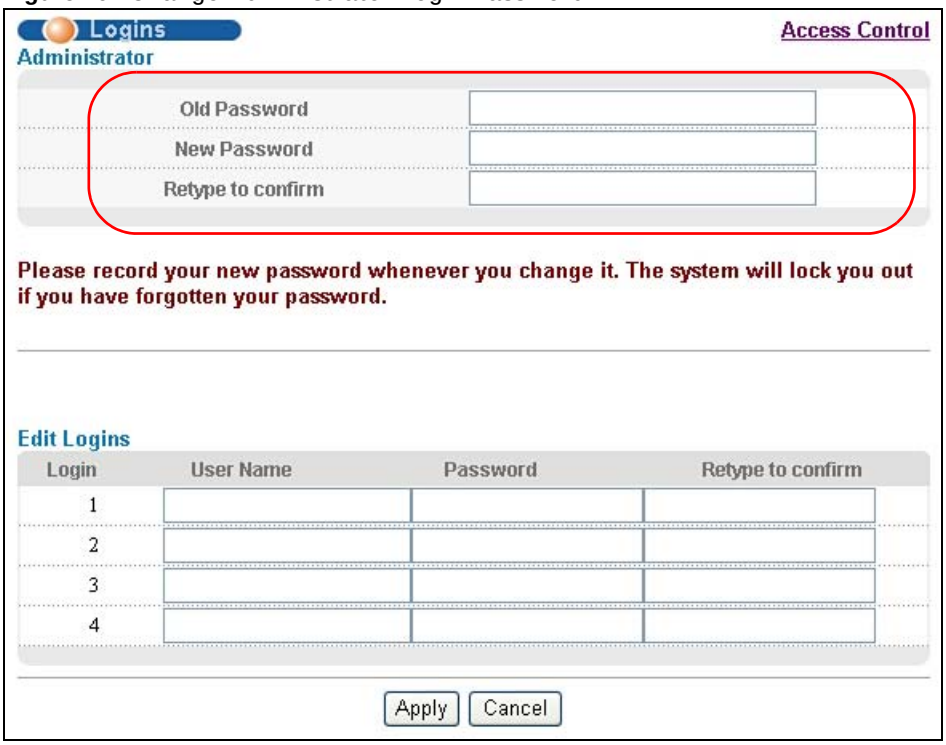
Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
ARP Learning	This link takes you to a screen where you can configure ARP learning mode on a per-port basis.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to a screen where you can view system logs and test port(s).
Syslog	This link takes you to screens where you can setup system logs and a system log server.
Cluster Management	This link takes you to screens where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to other ports.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management** > **Access Control** > **Logins** to display the next screen.

Figure 20 Change Administrator Login Password



4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save** link in the upper right hand corner of the web configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.

Note: Use the **Save** link when you are done with a configuration session.

4.5 Switch Lockout

You could block yourself (and all others) from managing the Switch if you do one of the following:

1 Delete the management VLAN (default is VLAN 1).

2 Delete all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the Switch.

3 Filter all traffic to the CPU port.

4 Disable all ports.

5 Misconfigure the text configuration file.

6 Forget the password and/or IP address.

7 Prevent all services from accessing the Switch.

8 Change a service port number but forget it.

Note: Be careful not to lock yourself and others out of the Switch.

4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600 bps with 8 data bits, no parity, one stop bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

1 Connect to the console port using a computer with terminal emulation software.

2 Disconnect and reconnect the Switch’s power to begin a session. When you reconnect the Switch’s power, you will see the initial screen.

3 When you see the message “`Press any key to enter Debug Mode within 3 seconds ...`” press any key to enter debug mode.

4 Type `atlc` after the “`Enter Debug Mode`” message.

5 Wait for the “`Starting XMODEM upload`” message before activating XMODEM upload on your terminal.

6 After a configuration file upload, type `atgo` to restart the Switch.

The Switch is now reinitialized with a default configuration file including the default password of “1234”.

4.7 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

Figure 21 Web Configurator: Logout Screen

4.8 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

5

Initial Setup Example

5.1 Overview

This chapter shows how to set up the Switch for an example network.

The following lists the configuration steps for the initial setup:

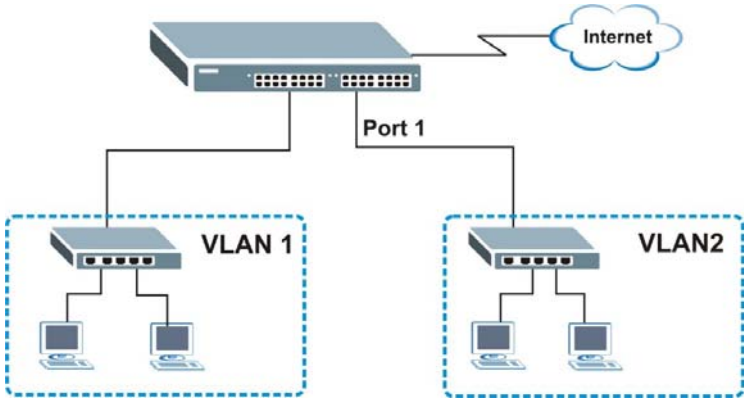
- Create a VLAN
- Set port VLAN ID
- Configure the Switch IP management address

5.1.1 Creating a VLAN

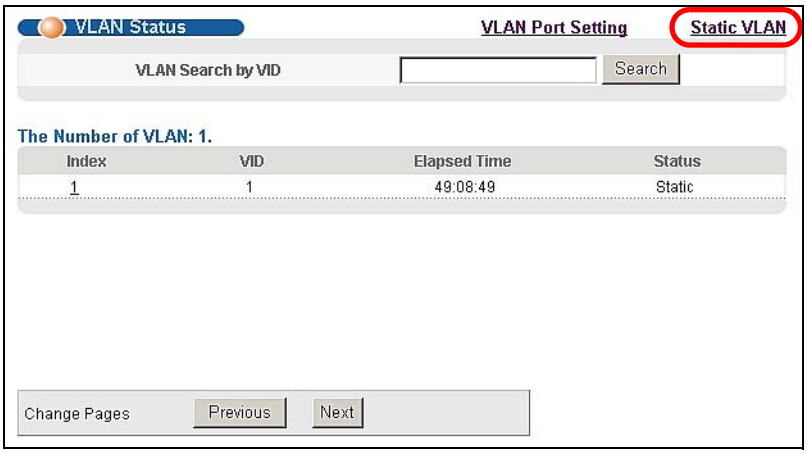
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 as a member of VLAN 2.

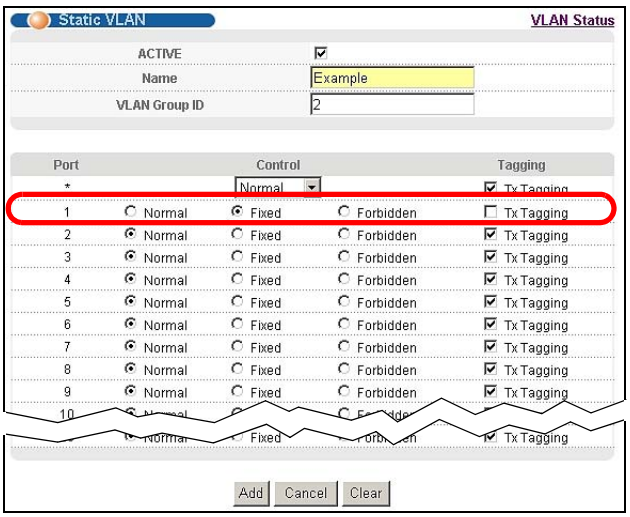
Figure 22 Initial Setup Network Example: VLAN



1 Click **Advanced Application** > **VLAN** in the navigation panel and click the **Static VLAN** link.



2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.



Note: The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.

4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

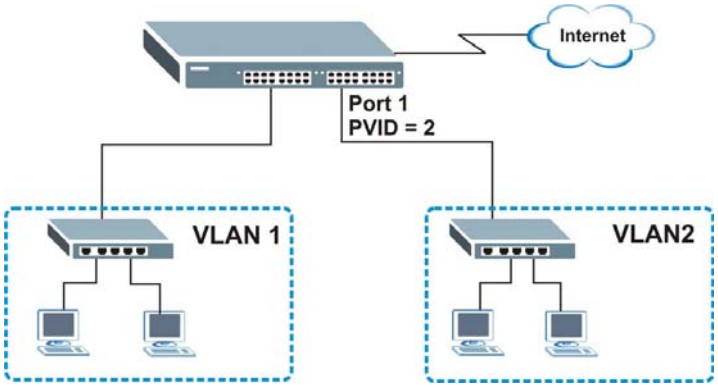
5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.2 Setting Port VID

Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

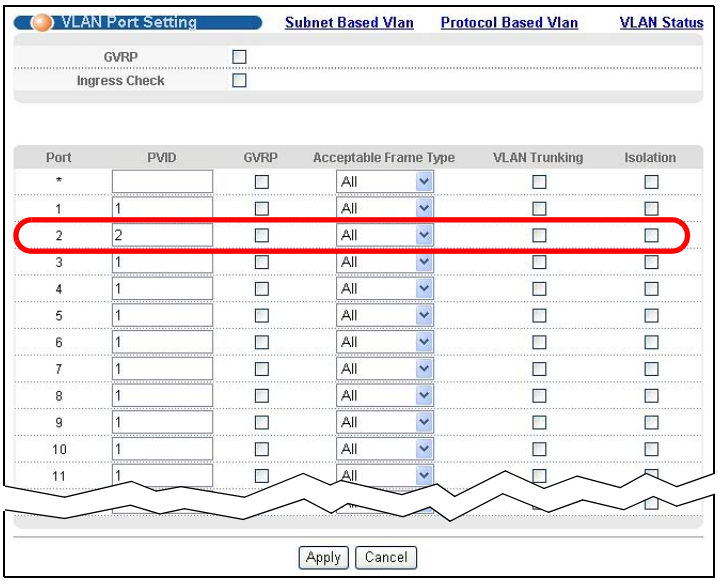
In the example network, configure 2 as the port VID on port 1 so that any untagged frames received on that port get sent to VLAN 2.

Figure 23 Initial Setup Network Example: Port VID



1 Click **Advanced Applications** > **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.

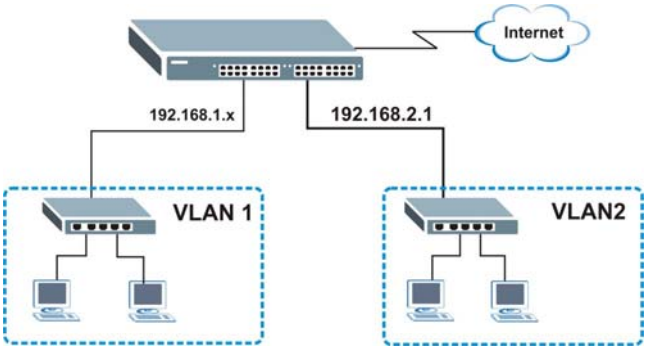
2 Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.



5.2 Configuring Switch Management IP Address

The default management IP address of the Switch is 192.168.1.1. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

Figure 24 Initial Setup Example: Management IP Address



1 Connect your computer to any Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.

2 Open your web browser and enter 192.168.1.1 (the default IP address) in the address bar to access the web configurator. See Section 4.2 on page 39 for more information.

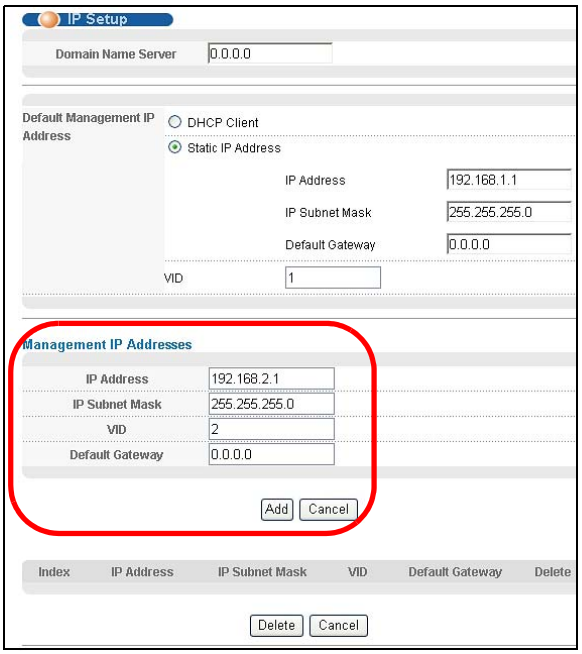
3 Click **Basic Setting** > **IP Setup** in the navigation panel.

4 Configure the related fields in the **IP Setup** screen.

5 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.

6 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.

7 Click **Add** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.



6

Tutorials

6.1 Overview

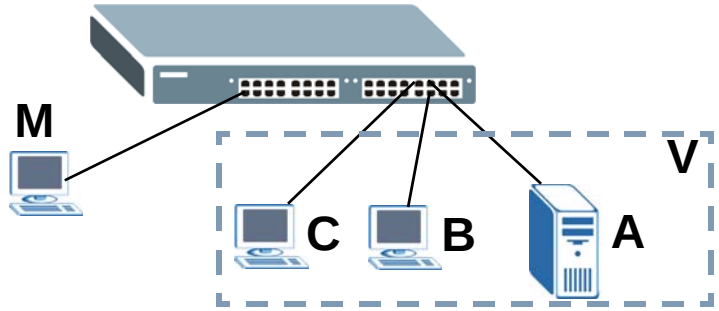
This chapter provides some examples of using the web configurator to set up and use the Switch. The tutorials include:

- How to Use DHCP Snooping on the Switch
- How to Use DHCP Relay on the Switch

6.2 How to Use DHCP Snooping on the Switch

You only want DHCP server **A** connected to port 5 to assign IP addresses to all devices in VLAN network (**V**). Create a VLAN containing ports 5, 6 and 7. Connect a computer **M** to the Switch for management.

Figure 25 Tutorial: DHCP Snooping Tutorial Overview



Note: For related information about DHCP snooping, see Section 25.1 on page 193.

The settings in this tutorial are as the following.

Table 6 Tutorial: Settings in this Tutorial

HOST	PORT CONNECTED	VLAN	PVID	DHCP SNOOPING PORT TRUSTED
DHCP Server (**A**)	5	1 and 100	100	Yes
DHCP Client (**B**)	6	1 and 100	100	No
DHCP Client (**C**)	7	1 and 100	100	No

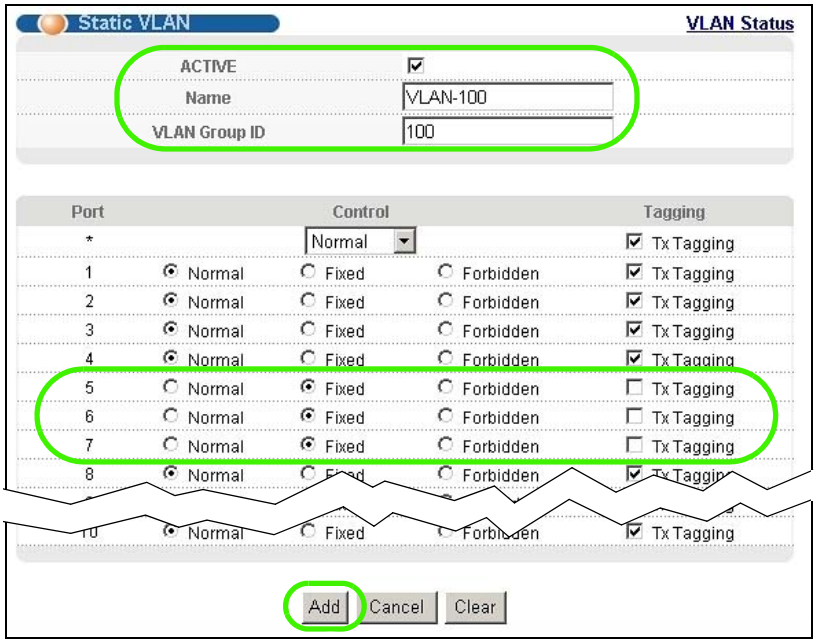
1 Access the Switch through **http://192.168.1.1** by default. Log into the Switch by entering the username (default: **admin**) and password (default: **1234**).

2 Go to **Advanced Application** > **VLAN** > **Static VLAN**, and create a VLAN with ID of 100. Add ports 5, 6 and 7 in the VLAN by selecting **Fixed** in the **Control** field as shown.

Deselect **Tx Tagging** because you don't want outgoing traffic to contain this VLAN tag.

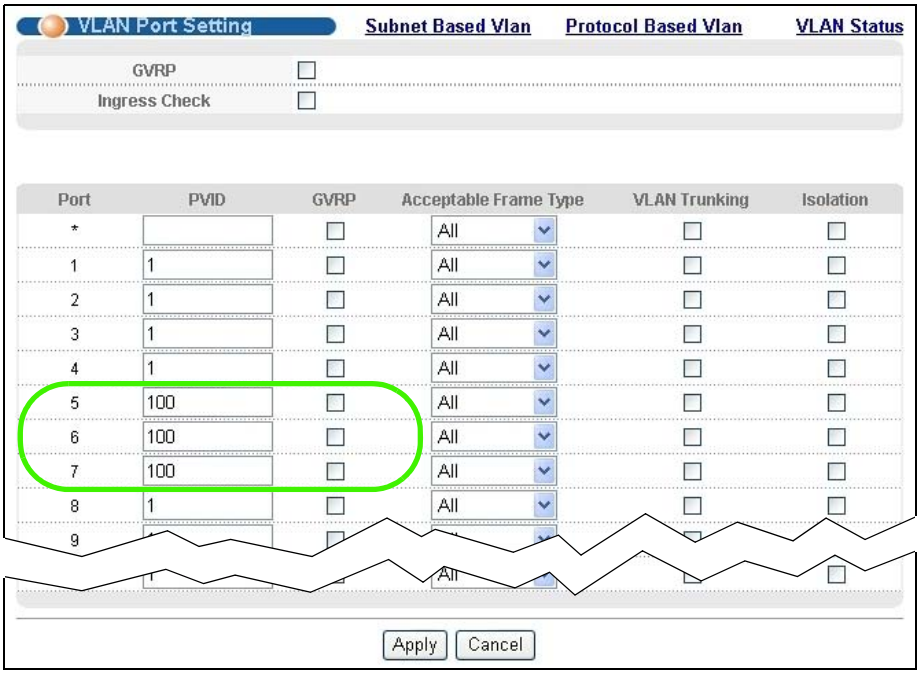
Click **Add**.

Figure 26 Tutorial: Create a VLAN and Add Ports to It



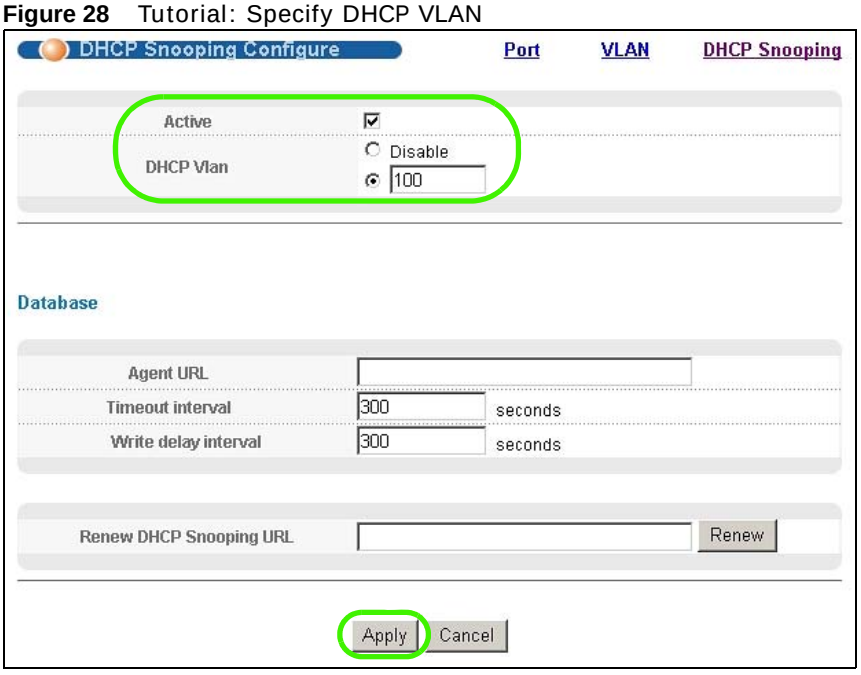
3 Go to **Advanced Application** > **VLAN** > **VLAN Port Setting**, and set the PVID of the ports 5, 6 and 7 to 100. This tags untagged incoming frames on ports 5, 6 and 7 with the tag 100.

Figure 27 Tutorial: Tag Untagged Frames



4 Go to **Advanced Application** > **IP Source Guard** > **DHCP snooping** > **Configure**, activate and specify VLAN 100 as the DHCP VLAN as shown. Click **Apply**.

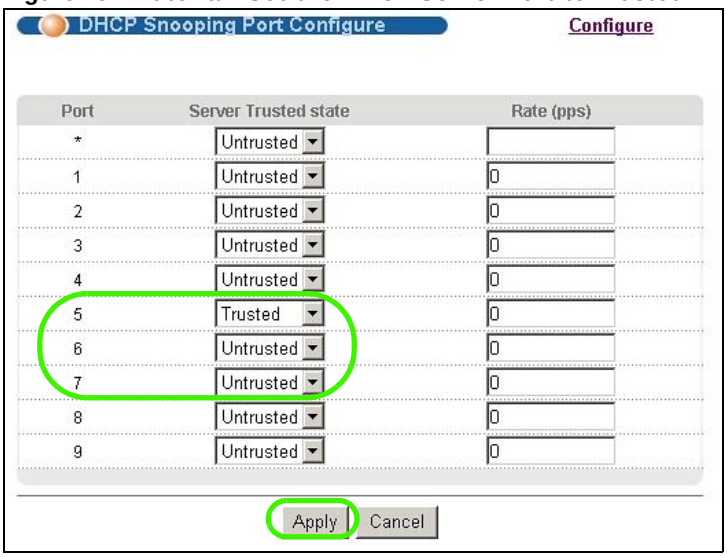
Figure 28 Tutorial: Specify DHCP VLAN



5 Click the **Port** link at the top right corner.

6 The **DHCP Snooping Port Configure** screen appears. Select **Trusted** in the **Server Trusted state** field for port 5 because the DHCP server is connected to port 5. Keep ports 6 and 7 **Untrusted** because they are connected to DHCP clients. Click **Apply**.

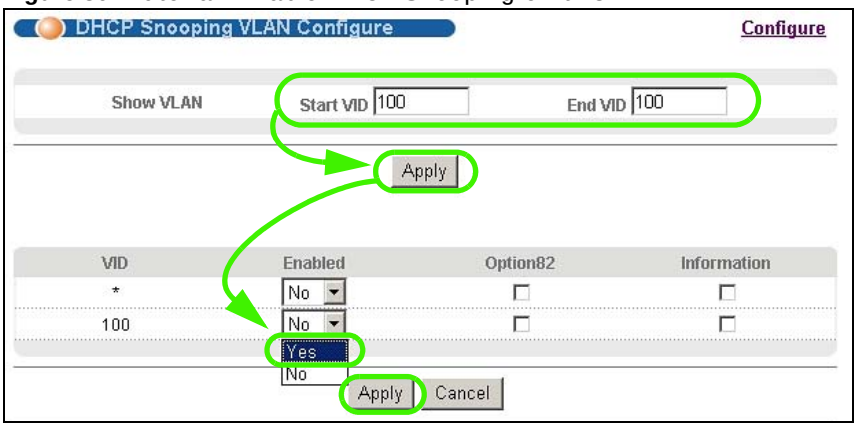
Figure 29 Tutorial: Set the DHCP Server Port to Trusted



7 Go to **Advanced Application** > **IP Source Guard** > **DHCP snooping** > **Configure** > **VLAN**, show VLAN 100 by entering 100 in the **Start VID** and **End VID** fields and click **Apply**. Then select **Yes** in the **Enabled** field of the VLAN 100 entry shown at the bottom section of the screen.

If you want to add more information in the DHCP request packets such as source VLAN ID or system name, you can also select the **Option82** and **Information** fields in the entry. See Section 25.10.1.3 on page 212.

Figure 30 Tutorial: Enable DHCP Snooping on this VLAN



8 Click **Save** at the top right corner of the web configurator to save the configuration permanently.

9 Connect your DHCP server to port 5 and a computer (as DHCP client) to either port 6 or 7. The computer should be able to get an IP address from the DHCP server. If you put the DHCP server on port 6 or 7, the computer will not able to get an IP address.

10 To check if DHCP snooping works, go to **Advanced Application** > **IP Source Guard**, you should see an IP assignment with the type **dhcp-snooping** as shown.

Figure 31 Tutorial: Check the Binding If DHCP Snooping Works

You can also telnet or log into the Switch's console. Use the command "show dhcp snooping binding" to see the DHCP snooping binding table as shown next.

```
sysname# show dhcp snooping binding
         MacAddress        IpAddress         Lease           Type  VLAN   Port
  -----------------  ---------------  ------------  -------------  ----  -----
  00:02:00:00:00:1c       10.10.1.16   6d23h59m20s  dhcp-snooping   100      7
  Total number of bindings: 1
```

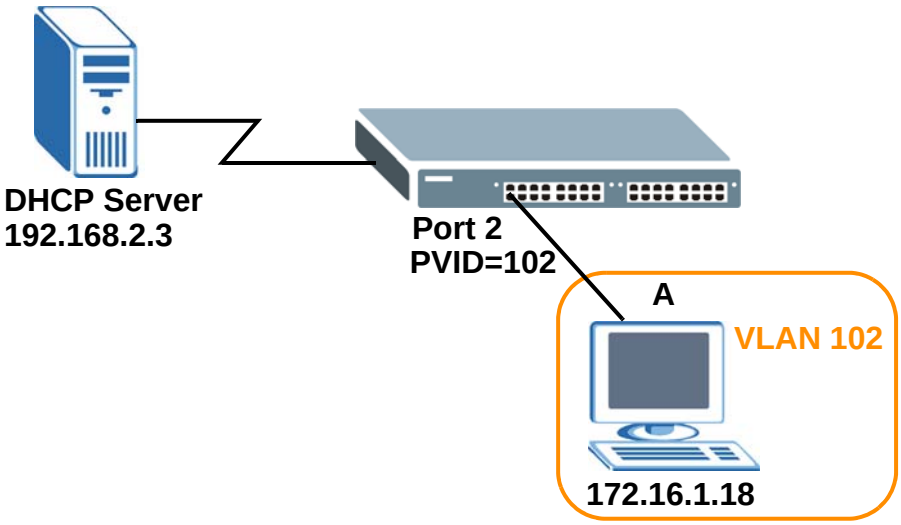
6.3 How to Use DHCP Relay on the Switch

This tutorial describes how to configure your Switch to forward DHCP client requests to a specific DHCP server. The DHCP server can then assign a specific IP address based on the information in the DHCP requests.

6.3.1 DHCP Relay Tutorial Introduction

In this example, you have configured your DHCP server (192.168.2.3) and want to have it assign a specific IP address (say 172.16.1.18) to DHCP client **A** based on the system name, VLAN ID and port number in the DHCP request. Client **A** connects to the Switch's port 2 in VLAN 102.

Figure 32 Tutorial: DHCP Relay Scenario



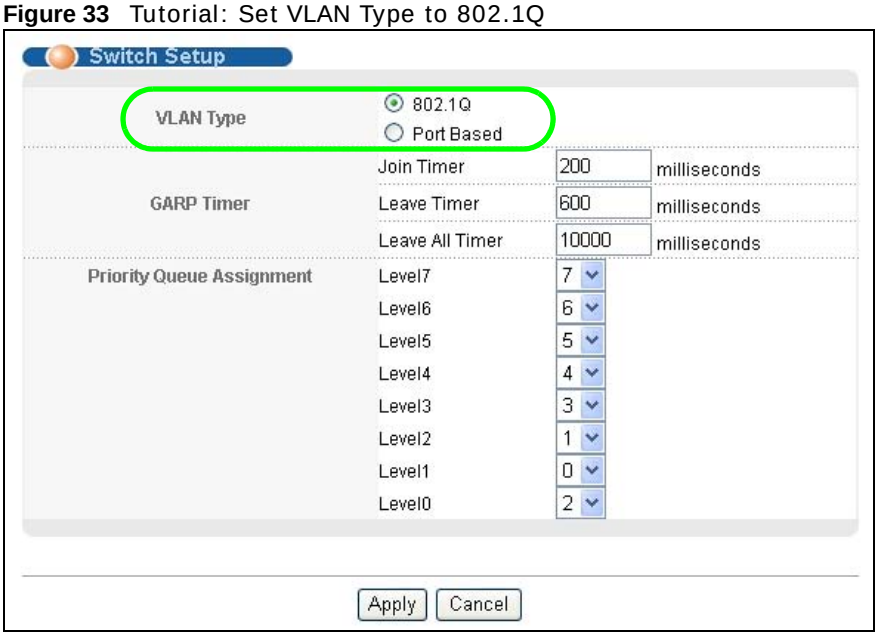
6.3.2 Creating a VLAN

Follow the steps below to configure port 2 as a member of VLAN 102.

1 Access the web configurator through the Switch's management port.

2 Go to **Basic Setting** > **Switch Setup** and set the VLAN type to **802.1Q**. Click **Apply** to save the settings to the run-time memory.

Figure 33 Tutorial: Set VLAN Type to 802.1Q



3 Click **Advanced Application** > **VLAN > Static VLAN**.

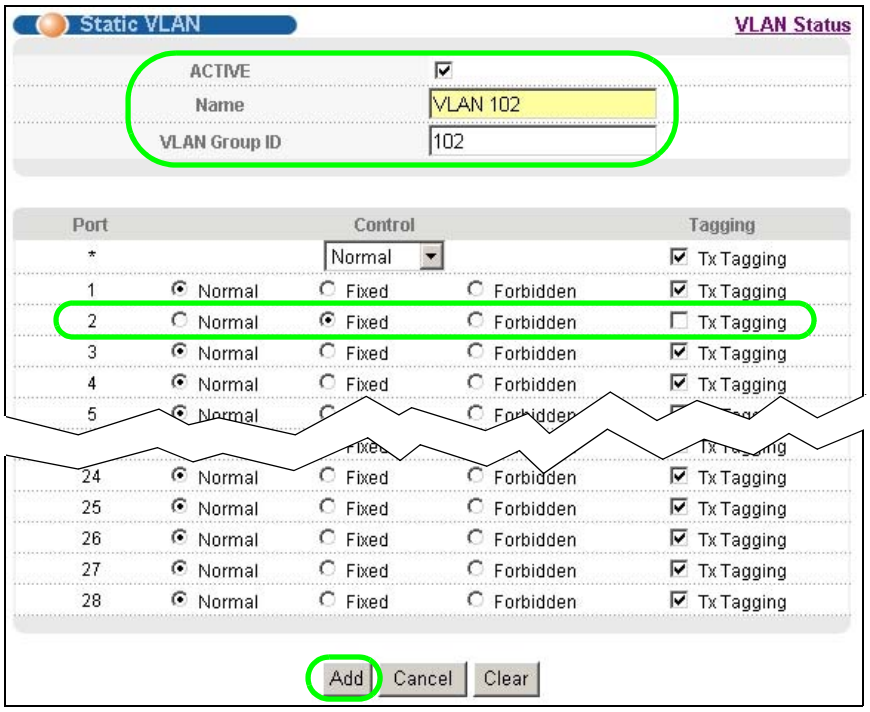
4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 102 for example) in the **Name** field and enter 102 in the **VLAN Group ID** field.

5 Select **Fixed** to configure port 2 to be a permanent member of this VLAN.

6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

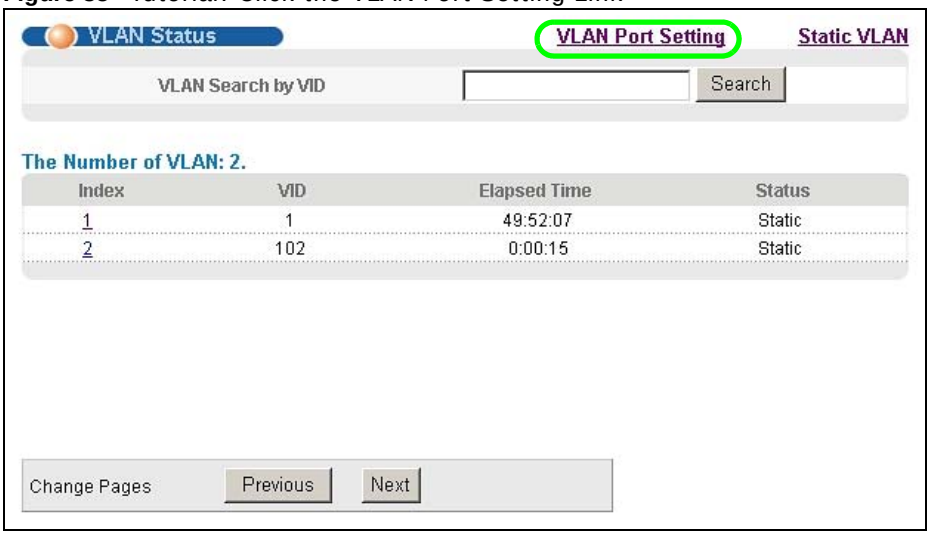
7 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Figure 34 Tutorial: Create a Static VLAN



8 Click the **VLAN Status** link in the **Static VLAN** screen and then the **VLAN Port Setting** link in the **VLAN Status** screen.

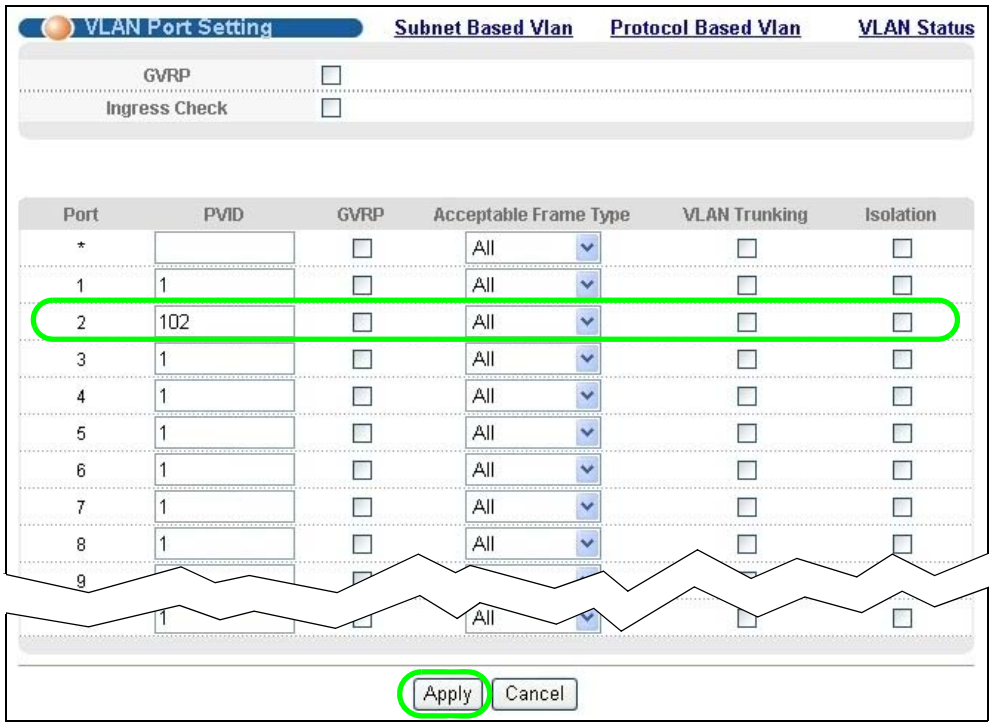
Figure 35 Tutorial: Click the VLAN Port Setting Link



9 Enter 102 in the **PVID** field for port 2 to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

10 Click **Apply** to save your changes back to the run-time memory.

Figure 36 Tutorial: Add Tag for Frames Received on Port 2



11 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

6.3.3 Configuring DHCP Relay

Follow the steps below to enable DHCP relay on the Switch and allow the Switch to add relay agent information (such as the VLAN ID) to DHCP requests.

1 Click **IP Application > DHCP** and then the **Global** link to open the **DHCP Relay** screen.

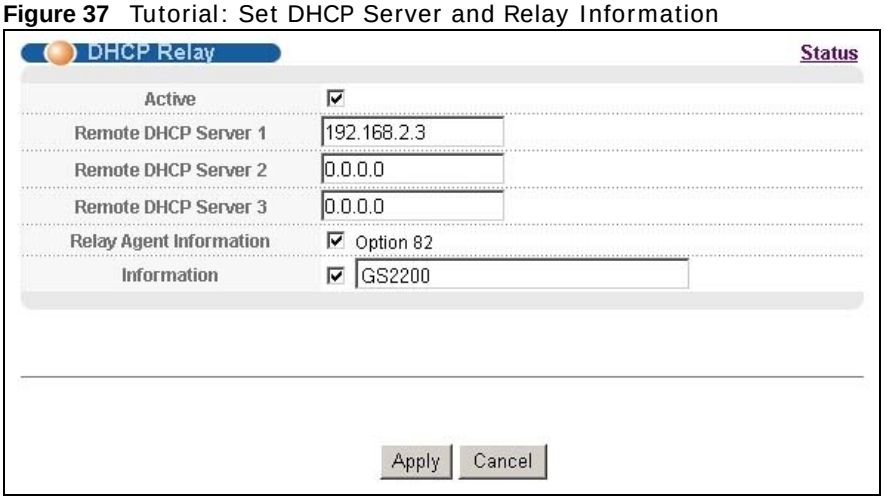
2 Select the **Active** check box.

3 Enter the DHCP server's IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.

4 Select the **Option 82** and the **Information** check boxes.

5 Click **Apply** to save your changes back to the run-time memory.

Figure 37 Tutorial: Set DHCP Server and Relay Information



6 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

7 The DHCP server can then assign a specific IP address based on the DHCP request.

6.3.4 Troubleshooting

Check the client **A**'s IP address. If it did not receive the IP address 172.16.1.18, make sure:

1 Client **A** is connected to the Switch's port 2 in VLAN 102.

2 You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the Switch.

3 You clicked the **Save** link on the Switch to have your settings take effect.

7

System Status and Port Statistics

7.1 Overview

This chapter describes the screens for system status (web configurator home page), port details and PoE status.

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

7.1.1 What You Can Do

- Use the **Port Status Summary** screen (Section 7.2 on page 61) to view the port statistics.
- Use the **Port Details** screen (Section 7.2.1 on page 63) to display individual port statistics.

7.2 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Status** screen as shown next.

Figure 38 Status (GS2200-24)

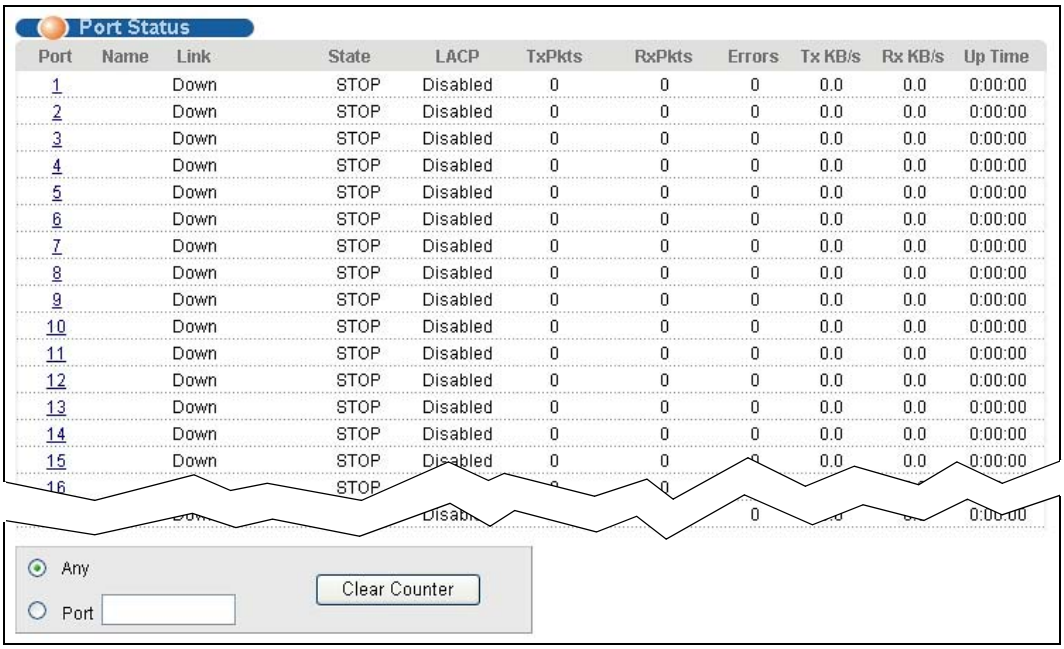
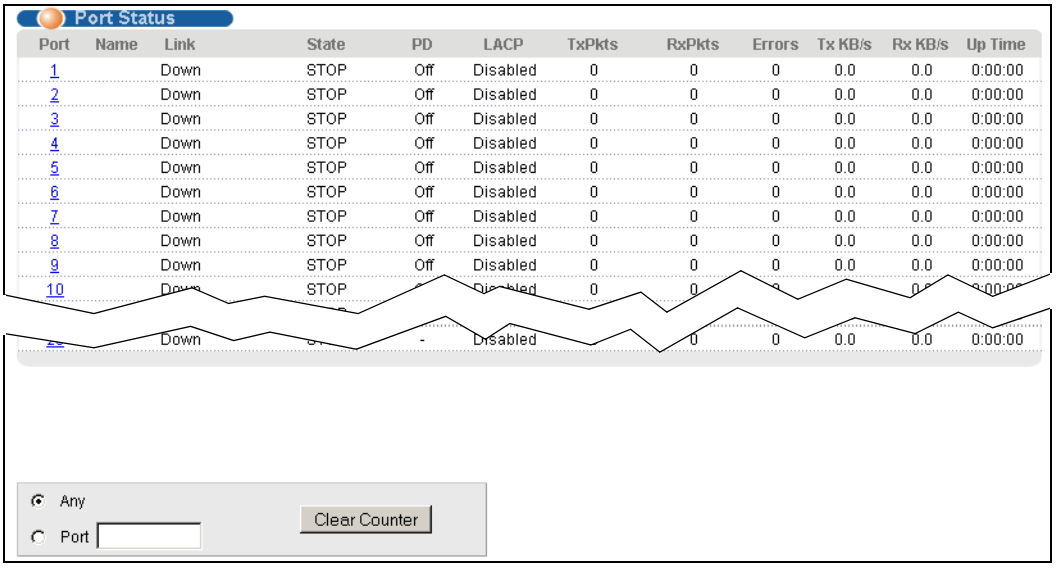


Figure 39 Status (GS2200-24P)



The following table describes the labels in this screen.

Table 7 Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to Figure 40 on page 63).
Name	This is the name you assigned to this port in the **Basic Setting** > **Port Setup** screen.

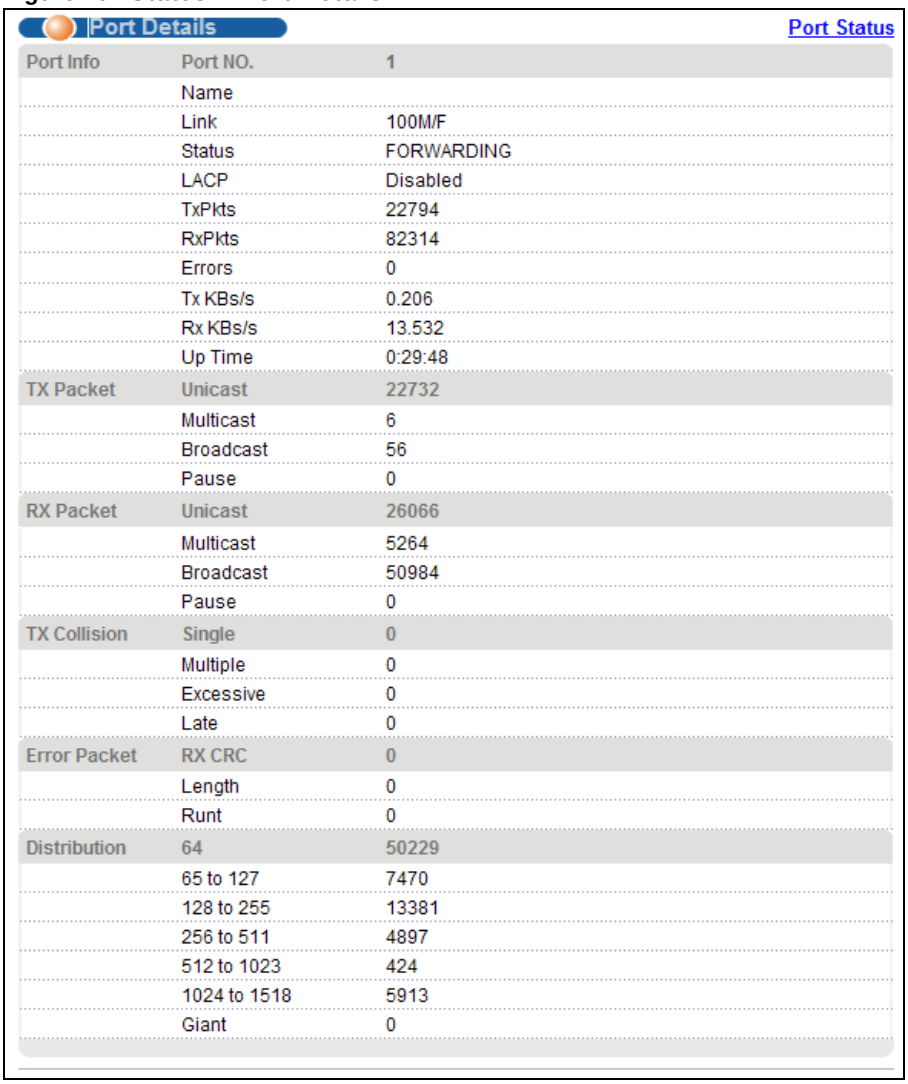
Table 7 Status (continued)

LABEL	DESCRIPTION
Link	This field displays the speed (either **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half). It also shows the cable type (**Copper** or **Fiber**) for the combo ports.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 13.1 on page 109 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
PD	(For GS2200-8HP or GS2200-24P only) This field displays whether or not a powered device (PD) is allowed to receive power from the Switch on this port.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Enter a port number and then click **Clear Counter** to erase the recorded statistical information for that port, or select **Any** to clear statistics for all ports.

7.2.1 Status: Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the Switch.

Figure 40 Status > Port Details



Port Info	Port NO.	1
	Name	
	Link	100M/F
	Status	FORWARDING
	LACP	Disabled
	TxPkts	22794
	RxPkts	82314
	Errors	0
	Tx KBs/s	0.206
	Rx KBs/s	13.532
	Up Time	0:29:48
TX Packet	Unicast	22732
	Multicast	6
	Broadcast	56
	Pause	0
RX Packet	Unicast	26066
	Multicast	5264
	Broadcast	50984
	Pause	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
Distribution	64	50229
	65 to 127	7470
	128 to 255	13381
	256 to 511	4897
	512 to 1023	424
	1024 to 1518	5913
	Giant	0

The following table describes the labels in this screen.

Table 8 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half duplex). It also shows the cable type (**Copper** or **Fiber**).

Table 8 Status: Port Details (continued)

LABEL	DESCRIPTION
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 13.1 on page 109 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about packets transmitted.	
Unicast	This field shows the number of good unicast packets transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Rx Packet The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.

Table 8 Status: Port Details (continued)

LABEL	DESCRIPTION
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your switch model. See Chapter 43 on page 307.

8

Basic Setting

8.1 Overview

This chapter describes how to configure the **System Info**, **General Setup**, **Switch Setup**, **IP Setup**, **Port Setup**, and **PoE** screens.

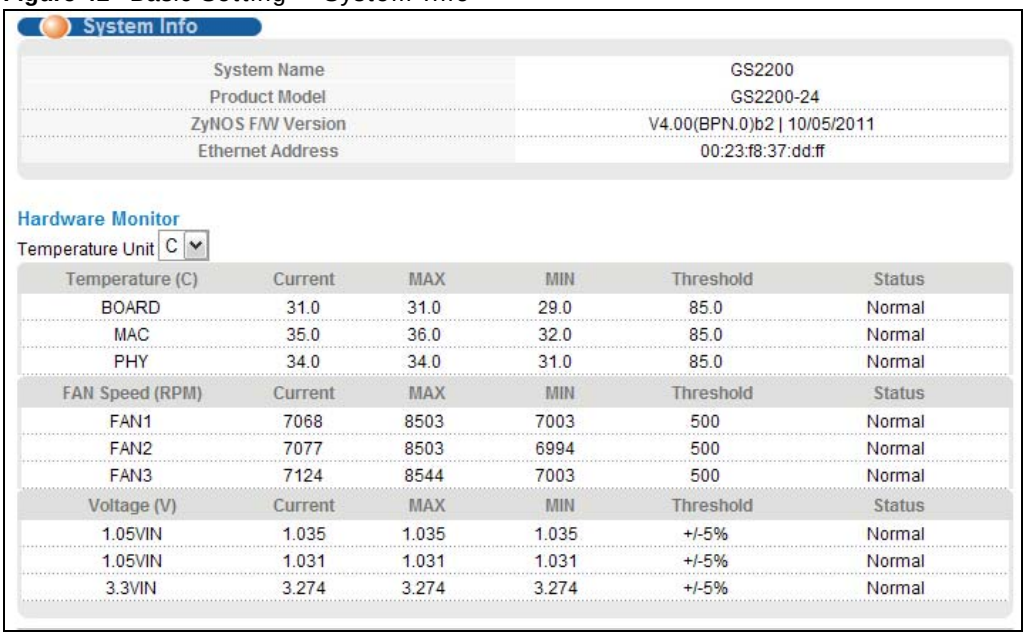
8.1.1 What You Can Do

- Use the **System Info** screen (Section 8.2 on page 67) to check the firmware version number.
- Use the **General Setup** screen (Section 8.3 on page 69) to configure general settings such as the system name and time.
- Use the **Switch Setup** screen (Section 8.5 on page 71) to choose your VLAN type, set the ARP aging time and GARP timers and assign priorities to queues.
- Use the **IP Setup** screen (Section 8.6.1 on page 73) to configure the Switch IP address, default gateway device, the default domain name server and the management VLAN ID.
- Use the **Port Setup** screen (Section 8.7 on page 75) to configure Switch port settings.
- Use the **PoE Status** screen (Section 8.8 on page 76) to view the current amount of power that PDs are receiving from the Switch and use the **PoE Setup** screen (Section 8.8.1 on page 79) to set the priority levels for the Switch in distributing power to PDs. (These screens are available to GS2200-8HP and GS2200-24P only.)

8.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. You can check the firmware version number.

Figure 41 Basic Setting > System Info



The following table describes the labels in this screen.

Table 9 Basic Setting > System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
Product Model	This field displays the product model of the Switch. Use this information when searching for firmware upgrade or looking for other support information in the website.
ZyNOS F/W Version	This field displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**BOARD**, **MAC** and **PHY** refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.

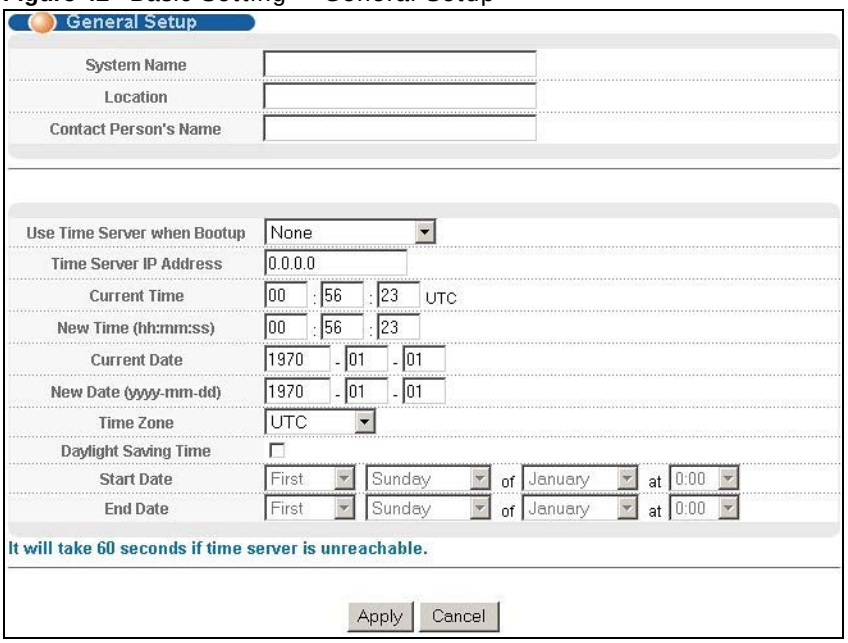
Table 9 Basic Setting > System Info (continued)

LABEL	DESCRIPTION
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown. Note: The fan speed information is available only on the GS2200-8HP and GS2200-24P that have fans.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.

8.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting** > **General Setup** in the navigation panel to display the screen as shown.

Figure 42 Basic Setting > General Setup



The following table describes the labels in this screen.

Table 10 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC 867)** format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None** is the default value. Enter the time manually. Each time you turn on the Switch, the time and date will be reset to 1970-1-1 0:0:0.
Time Server IP Address	Enter the IP address of your timeserver. The Switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).

Table 10 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

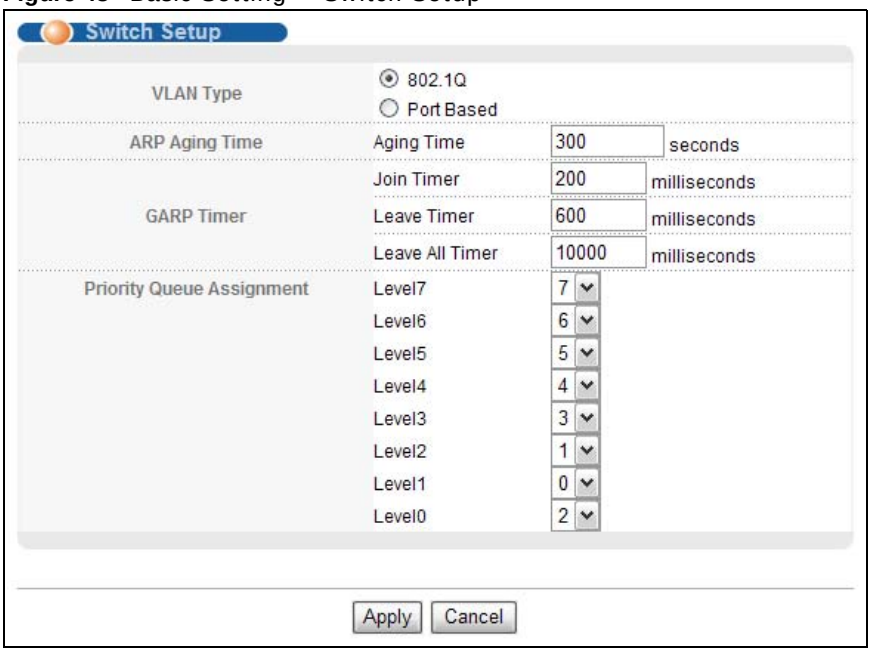
Note: VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 9 on page 83 for information on port-based and 802.1Q tagged VLANs.

8.5 Switch Setup Screen

Click **Basic Setting** > **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to Chapter 9 on page 83 for more information on VLAN.

Figure 43 Basic Setting > Switch Setup



The following table describes the labels in this screen.

Table 11 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose **802.1Q** or **Port Based**. The **VLAN Setup** screen changes depending on whether you choose **802.1Q** VLAN type or **Port Based** VLAN type in this screen. See Chapter 9 on page 83 for more information.
ARP Aging Time	Enter a time from 60 to 1000000 seconds. This is how long a dynamically learned ARP entry can remain in the ARP table before it is cleared (and must be relearned).
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	

Table 11 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a **Join Period** timer. The allowed **Join Time** range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Time sets the duration of the **Leave Period** timer for GVRP in milliseconds. Each port has a single **Leave Period** timer. Leave Time must be two times larger than **Join Timer**; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

8.6 IP Setup

Use the **IP Setup** screen to configure the Switch IP address, default gateway device, the default domain name server and the management VLAN ID. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

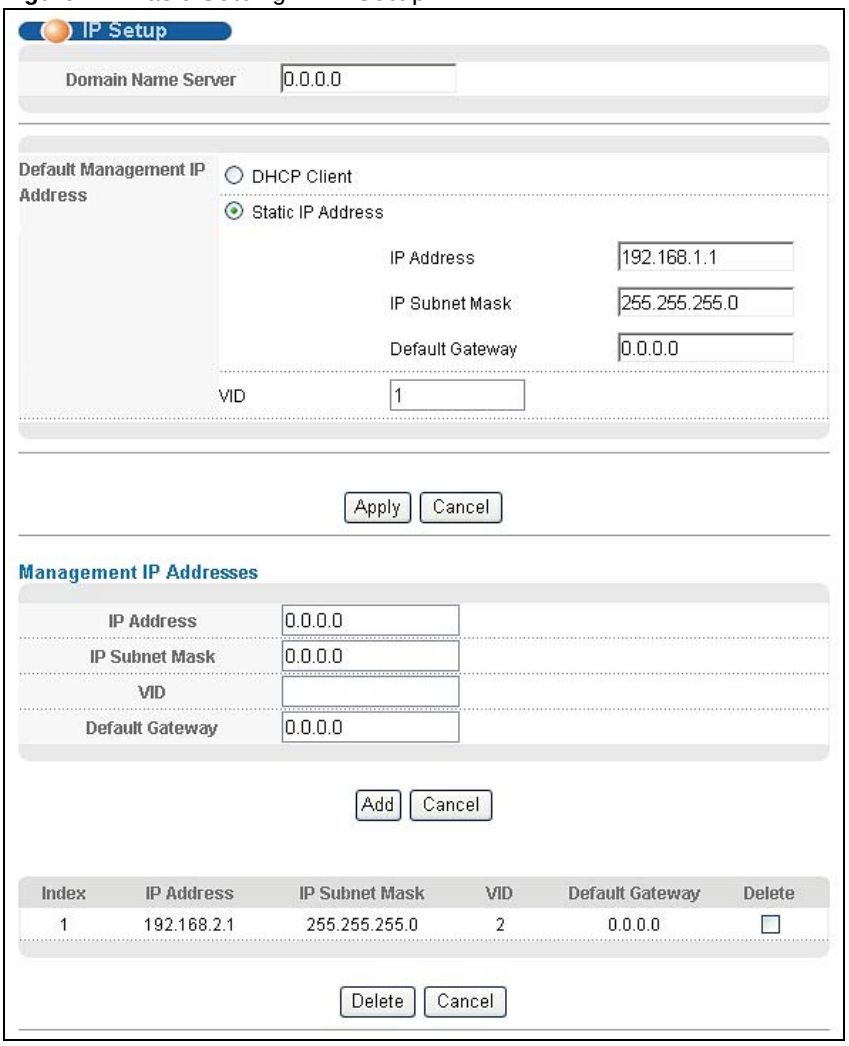
8.6.1 Management IP Addresses

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

You can configure up to 64 IP addresses which are used to access and manage the Switch from the ports belonging to the pre-defined VLAN(s).

Note: You must configure a VLAN first.

Figure 44 Basic Setting > IP Setup



The following table describes the labels in this screen.

Table 12 Basic Setting > IP Setup

LABEL	DESCRIPTION
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Default Management IP Address	

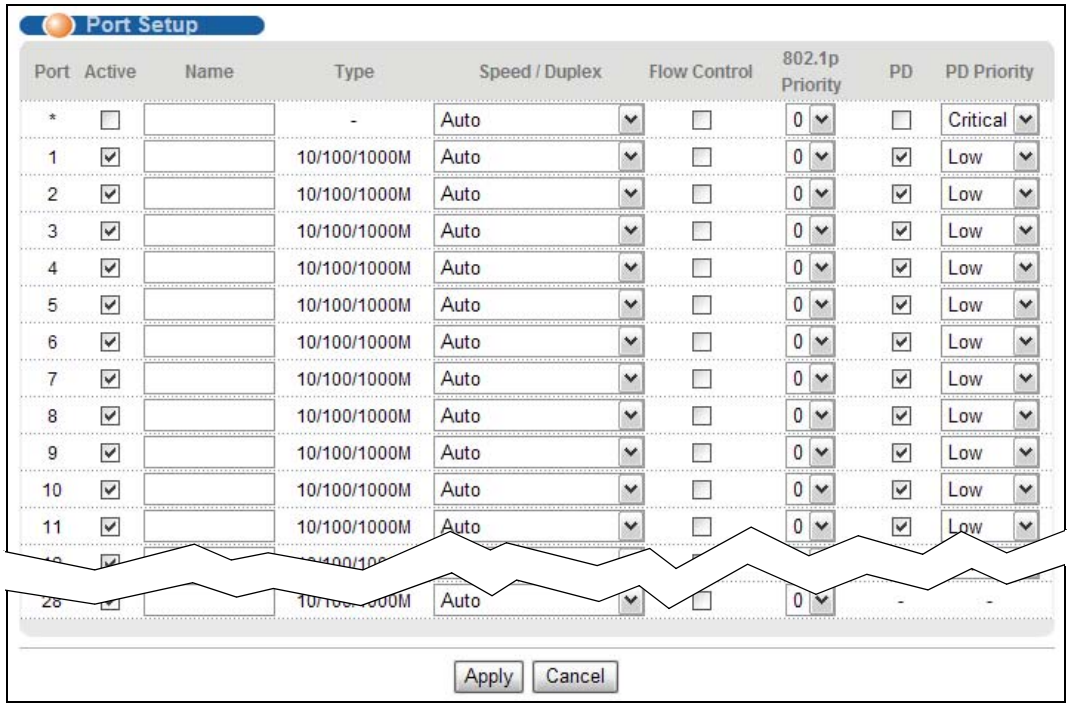
Table 12 Basic Setting > IP Setup (continued)

LABEL	DESCRIPTION
DHCP Client	Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
VID	Enter the VLAN identification number associated with the Switch IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the Switch make sure the port that you are connected to is a member of Management VLAN.
Management IP Addresses You can create up to 64 IP addresses, which are used to access and manage the Switch from the ports belonging to the pre-defined VLAN(s). You must configure a VLAN first.	
IP Address	Enter the IP address for managing the Switch by the members of the VLAN specified in the **VID** field below.
IP Subnet Mask	Enter the IP subnet mask in dotted decimal notation.
VID	Type the VLAN group identification number.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.
Add	Click **Add** to insert the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Index	This field displays the index number of the rule. Click an index number to edit the rule.
IP Address	This field displays the IP address.
IP Subnet Mask	This field displays the subnet mask.
VID	This field displays the ID number of the VLAN group.
Default Gateway	This field displays the IP address of the default gateway.
Delete	Check the management IP addresses that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes in the **Delete** column.

8.7 Port Setup

Use this screen to configure Switch port settings. Click **Basic Setting** > **Port Setup** in the navigation panel to display the configuration screen.

Figure 45 Basic Setting > Port Setup



The following table describes the labels in this screen.

Table 13 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some web configurator screens.
Type	This field displays **10/100M** for Fast Ethernet connections and **10/100/1000M** for Gigabit connections.

Table 13 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex**, **100M/Full Duplex** and **1000M/Full Duplex** (Gigabit connections only). Selecting **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select **Flow Control** to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in Table 11 on page 71 for more information.
PD	Select this to provide power to a PD connected to the port. If left unchecked, the PD connected to the port cannot receive power from the Switch.
PD Priority	This field is only available on the model that supports PoE but not available for the Dual Personality Interfaces. When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority. Select **Critical** to give the highest PD priority on the port. Select **High** to set the Switch to assign the remaining power to the port after all critical priority ports are served. Select **Low** to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.8 PoE Status

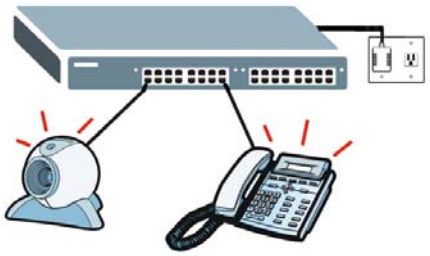
Note: The following screens are available for the GS2200-8HP or GS2200-24P model only. Some features are only available for the Ethernet ports (1 to 8 or 1 to 24).

The GS2200-8HP supports the IEEE 802.3at High Power over Ethernet (PoE) standard and the GS2200-24P supports the IEEE 802.3af PoE standard.

A powered device (PD) is a device such as an access point or a switch, that supports PoE (Power over Ethernet) so that it can receive power from another device through an Ethernet port.

In the figure below, the IP camera and IP phone get their power directly from the Switch. Aside from minimizing the need for cables and wires, PoE removes the hassle of trying to find a nearby electric outlet to power up devices.

Figure 46 Powered Device Examples



You can also set priorities so that the Switch is able to reserve and allocate power to certain PDs.

Note: The GS2200-8HP complies with the IEEE 802.3at High Power over Ethernet (PoE) standard and the GS2200-24P complies with the IEEE 802.3af PoE standard. Ports 1 to 4 on the GS2200-8HP can supply power of up to 30W per Ethernet port. Ports 5 to 8 on the GS2200-8HP and ports 1 to 24 on the GS2200-24P can supply power of up to 15.4W per Ethernet port.

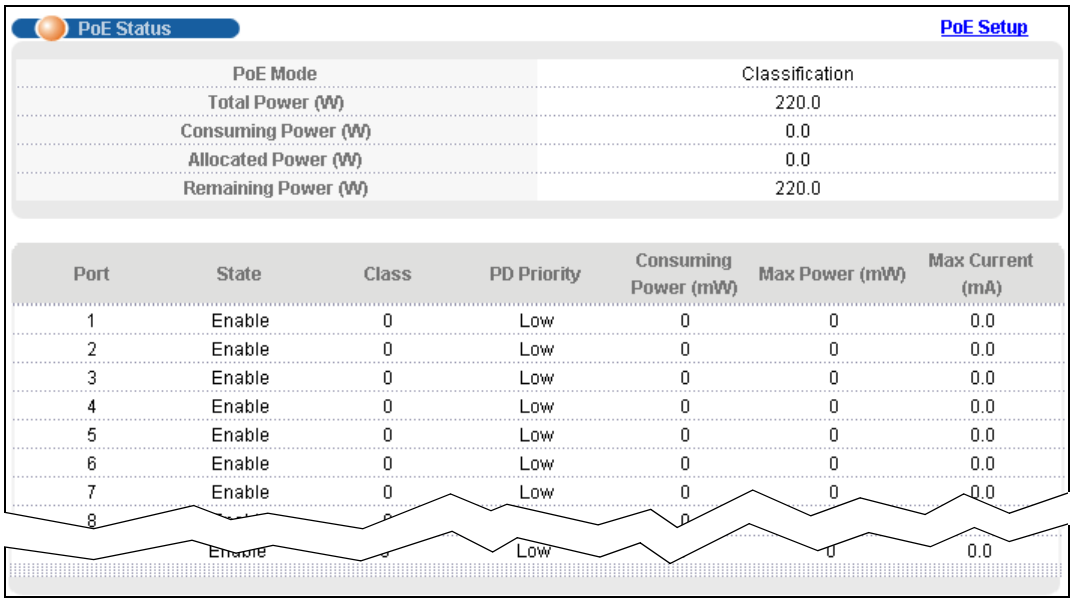
Note: The GS2200-24P is compatible with ZyXEL's PPS250 power module. The PPS250 provides additional external PoE power budget on top of the internal power budget of the GS2200-24P. Refer to the User's Guide of the PPS250 for more information.

Note: The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors. The Switch is to be connected only to PoE networks without routing to the outside plant.

Note: The RPS connector port at the back panel of the GS2200-24P and RPS connector cable should only be used with the PPS250. Do not insert other connector cables to the RPS connector port of the GS2200-24P or the PPS250.

To view the current amount of power that PDs are receiving from the Switch, click **Basic Setting** > **PoE**.

Figure 47 Basic Setting > PoE Status



The following table describes the labels in this screen.

Table 14 Basic Setting > PoE Status

LABEL	DESCRIPTION
PoE Status	
PoE Mode	This field displays the power management mode used by the Switch, whether it is in **Classification** or **Consumption** mode.
Total Power	This field displays the total power the Switch can provide to the connected PoE-enabled devices on the PoE ports.
Consuming Power (W)	This field displays the amount of power the Switch is currently supplying to the connected PoE-enabled devices.
Allocated Power (W)	This field displays the total amount of power the Switch has reserved for PoE after negotiating with the connected PoE device(s). It shows **NA** when the Switch is in **Consumption** mode. **Consuming Power (W)** can be less than or equal but not more than the **Allocated Power (W)**.
Remaining Power (W)	This field displays the amount of power the Switch can still provide for PoE. Note: The GS2200-24P must have at least 20 W of remaining power in order to supply power to a PoE device, even if the PoE device needs less than 20 W.
Port	This is the port index number.
State	This field shows which ports can receive power from the Switch. You can set this in Section 8.8.1 on page 79. • **Disable** - The PD connected to this port cannot get power supply. • **Enable** - The PD connected to this port can receive power.

Table 14 Basic Setting > PoE Status (continued)

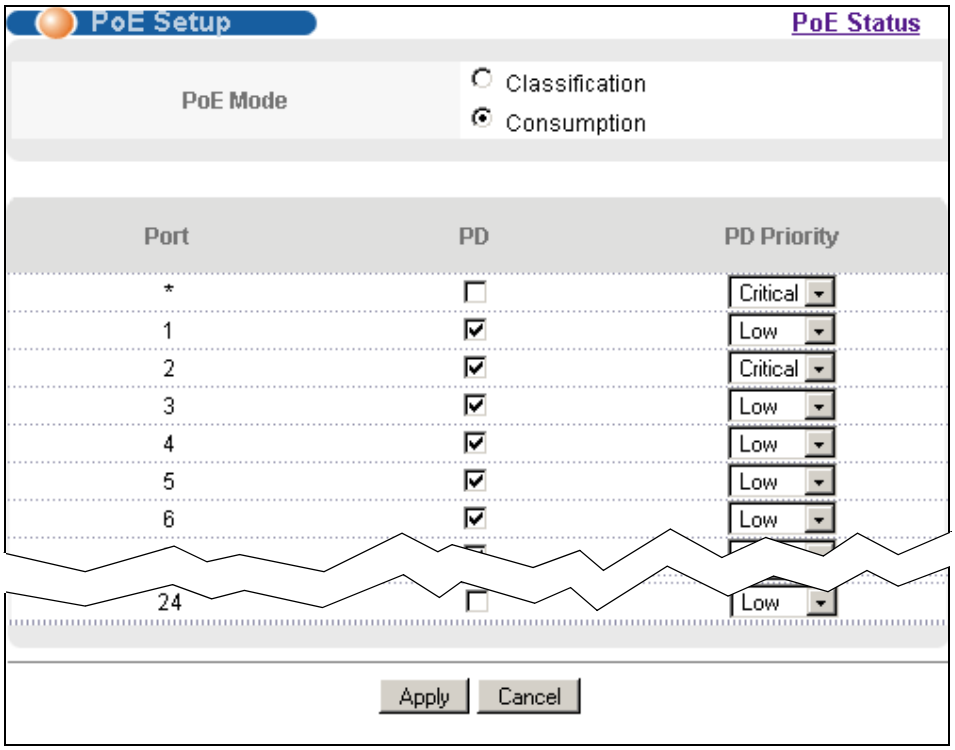
LABEL	DESCRIPTION
Class	This shows the IEEE 802.3af power classification of the PD. This is a number from 0 to 4, where each value represents a range of power (W) and power current (mA) that the PD requires to function. The ranges are as follows. • **Class 0** - Default, 0.44 to 12.94 • **Class 1** - Optional, 0.44 to 3.84 • **Class 2** - Optional , 3.84 to 6.49 • **Class 3** - Optional, 6.49 to 12.95 • **Class 4** - Reserved (PSEs classify as Class 0) in a Switch that supports IEEE 802.3af only. Optional, 12.95 to 25.50 in a Switch that supports IEEE 802.3at.
PD Priority	When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority first. • **Critical** has the highest priority. • **High** has the Switch assign power to the port after all critical priority ports are served. • **Low** has the Switch assign power to the port after all critical and high priority ports are served.
Consuming Power (mW)	This field displays the current amount of power consumed by the PD from the Switch on this port.
Max Power (mW)	This field displays the maximum amount of power the PD could use from the Switch on this port.
Max Current (mA)	This field displays the maximum amount of current drawn by the PD from the Switch on this port.

8.8.1 PoE Setup

Use this screen to set the priority levels for the Switch in distributing power to PDs.

Click the **PoE Setup** link in the **Basic Setting > PoE Status** screen. The following screen opens.

Figure 48 Basic Setting > PoE > PoE Setup



The following table describes the labels in this screen.

Table 15 Basic Setting > PoE > PoE Setup

LABEL	DESCRIPTION
PoE Mode	Select the power management mode you want the Switch to use. • **Classification** - Select this if you want the Switch to reserve the Max Power (mW) to each PD according to the power classification of the PD. If the total power supply runs out, PDs with lower priority do not get power to function. • **Consumption** - Select this if you want the Switch to manage the total power supply so that each connected PD gets a resource. However, the power allocated by the Switch may be less than the Max Power (mW) of the PD. PDs with higher priority also get more power than those with lower priority levels.
Port	This is the port index number.
PD	Select this to provide power to a PD connected to the port. If left unchecked, the PD connected to the port cannot receive power from the Switch.
PD Priority	This field is only available on the PWR model but not available for the Gigabit or mini-GBIC ports. When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority. Select **Critical** to give the highest PD priority on the port. Select **High** to set the Switch to assign the remaining power to the port after all critical priority ports are served. Select **Low** to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.

Table 15 Basic Setting > PoE > PoE Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9

VLAN

9.1 Overview

This chapter shows you how to configure 802.1Q tagged and port-based VLANs. The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen.

9.1.1 What You Can Do

- Use the **VLAN Status** screen (Section 9.2 on page 86) to view all VLAN groups.
- Use the **VLAN Detail** screen (Section 9.2.1 on page 87) to view detailed port settings and status of the VLAN group.
- Use the **Static VLAN** screen (Section 9.3 on page 88) to configure and view 802.1Q VLAN parameters for the Switch.
- Use the **VLAN Port Setting** screen (Section 9.4 on page 90) to configure the static VLAN (IEEE 802.1Q) settings on a port.
- Use the **Subnet Based VLAN** screen (Section 9.5 on page 91) to set up VLANs that allow you to group traffic into logical VLANs based on the source IP subnet you specify.
- Use the **Protocol Based VLAN** screen (Section 9.6 on page 94) to set up VLANs that allow you to group traffic into logical VLANs based on the protocol you specify.
- Use the **Port-Based VLAN** screen (Section 9.7 on page 96) to set up VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

9.1.2 What You Need to Know

Read this section to know more about VLAN and how to configure the screens.

IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority

level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

9.1.2.1 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local Switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 16 IEEE 802.1Q VLAN Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/ deregistration process.

Table 16 IEEE 802.1Q VLAN Terminology (continued)

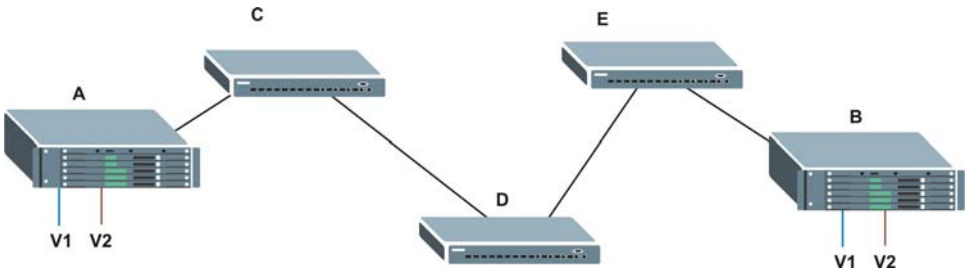
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member

9.1.2.2 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

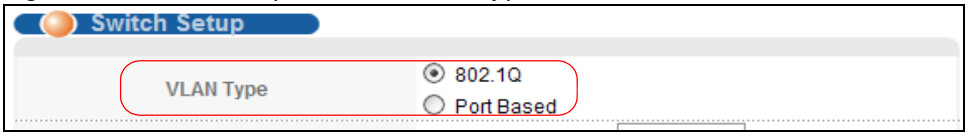
Figure 49 Port VLAN Trunking



9.1.2.3 Select the VLAN Type

Select a VLAN type in the **Basic Setting** > **Switch Setup** screen.

Figure 50 Switch Setup > Select VLAN Type



Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

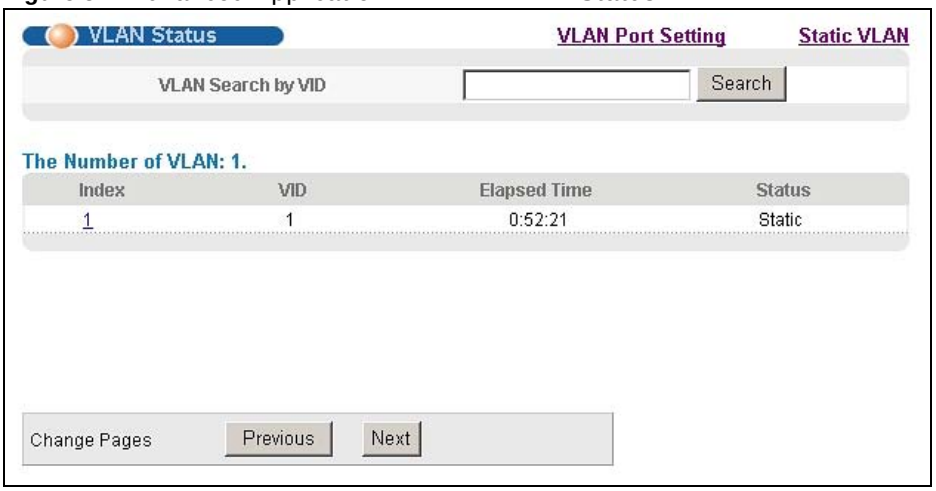
- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

9.2 VLAN Status

Click **Advanced Application** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 51 Advanced Application > VLAN: VLAN Status



The following table describes the labels in this screen.

Table 17 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click **Search** to display only the specified VLAN(s) in the list below. Leave this field blank and click **Search** to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the **Search** button to look for certain VLANs.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.

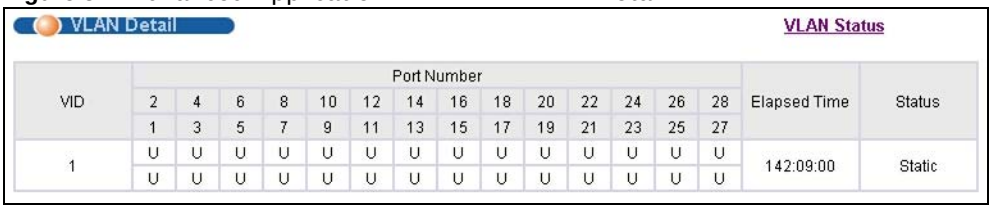
Table 17 Advanced Application > VLAN: VLAN Status (continued)

LABEL	DESCRIPTION
Status	This field shows how this VLAN was added to the Switch. **dynamic**: using GVRP **static**: added as a permanent entry
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

9.2.1 VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 52 Advanced Application > VLAN > VLAN Detail



The following table describes the labels in this screen.

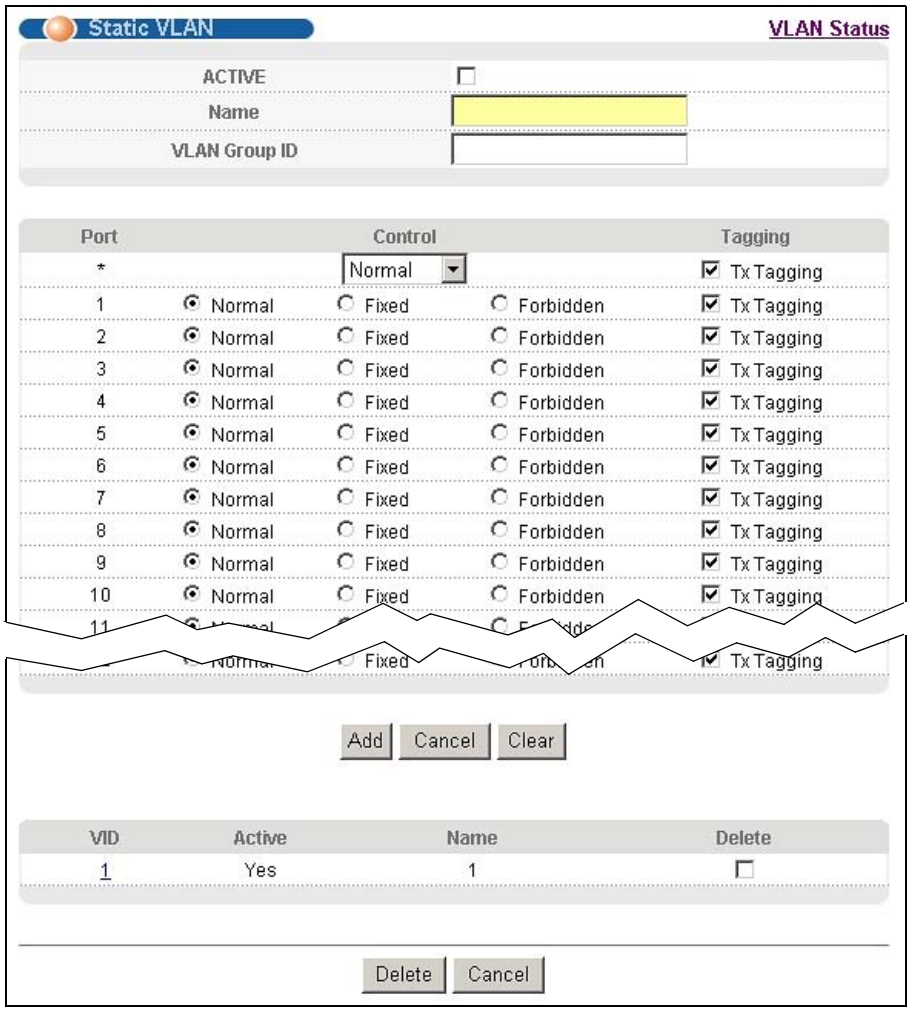
Table 18 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the **VLAN Status** screen.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. **dynamic**: using GVRP **static**: added as a permanent entry

9.3 Configure a Static VLAN

Use this screen to configure and view 802.1Q VLAN parameters for the Switch. To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 53 Advanced Application > VLAN > Static VLAN



The following table describes the related labels in this screen.

Table 19 Advanced Application > VLAN > Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.

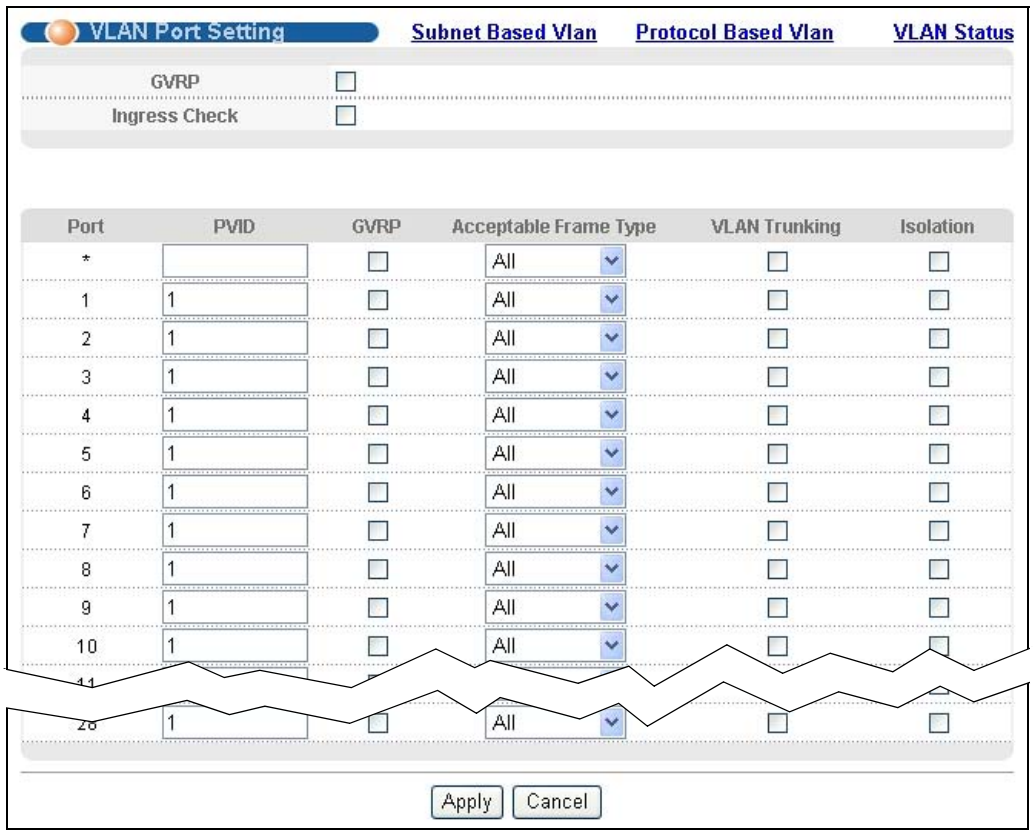
Table 19 Advanced Application > VLAN > Static VLAN (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to change the fields back to their last saved values.
Clear	Click **Clear** to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

9.4 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 54 Advanced Application > VLAN > VLAN Port Setting



The following table describes the labels in this screen.

Table 20 Advanced Application > VLAN > VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
Ingress Check	If this check box is selected, the Switch discards incoming frames on a port for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 20 Advanced Application > VLAN > VLAN Port Setting (continued)

LABEL	DESCRIPTION
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All**, **Tag Only** and **Untag Only**. Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames will be dropped. Select **Untag Only** to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable **VLAN Trunking** on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Isolation	Select this to allows this port to communicate only with the CPU management port and the ports on which the isolation feature is not enabled.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.5 Subnet Based VLANs

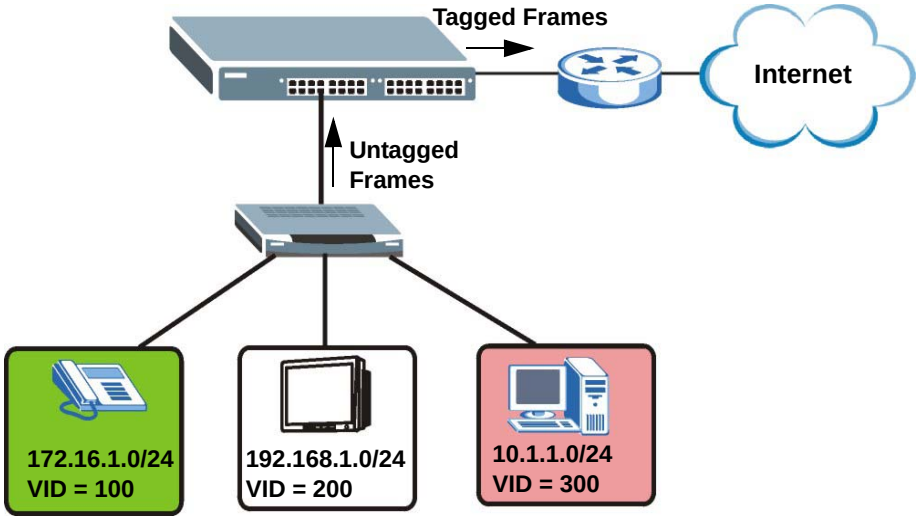
Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

For example, an ISP (Internet Services Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The Switch can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All

untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is video services receive the highest priority and data the lowest.

Figure 55 Subnet Based VLAN Application Example



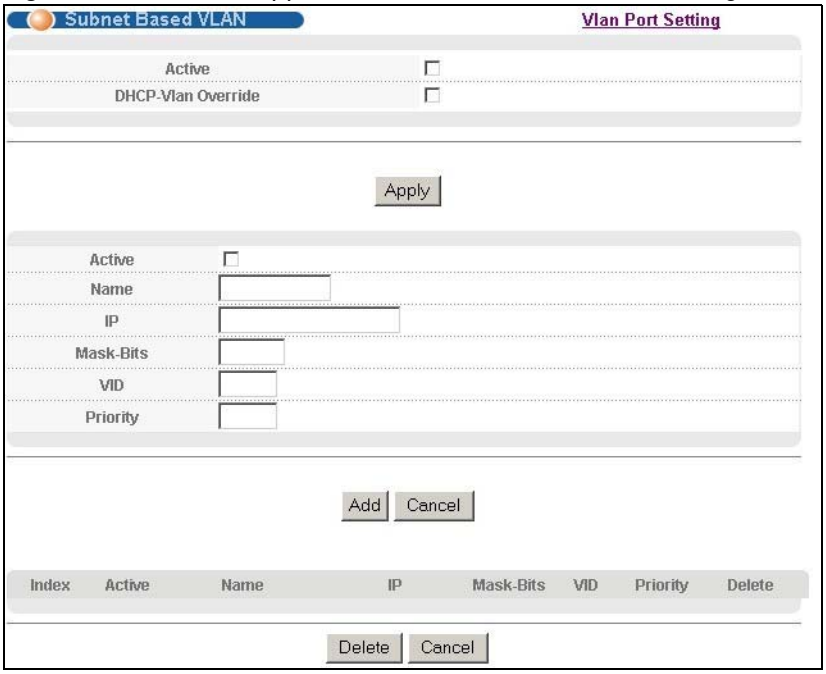
9.5.1 Configuring Subnet Based VLAN

Click **Subnet Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Note: Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

Note: You can not enable subnet-based VLANs on the Switch when the Guest VLAN feature is activated on a port.

Figure 56 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN



The following table describes the labels in this screen.

Table 21 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this subnet based VLANs on the Switch.
DHCP-Vlan Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN. Select this checkbox to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Active	Check this box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alpha numeric characters to identify this subnet based VLAN.
IP	Enter the IP address of the subnet for which you want to configure this subnet based VLAN.
Mask-Bits	Enter the bit number of the subnet mask. To find the bit number, convert the subnet mask to binary format and add all the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1s in binary. There are three 255s, so add three eights together and you get the bit number (24).
VID	Enter the ID of a VLAN with which the untagged frames from the IP subnet specified in this subnet based VLAN are tagged. This must be an existing VLAN which you defined in the **Advanced Applications** > **VLAN** screens.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Table 21 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

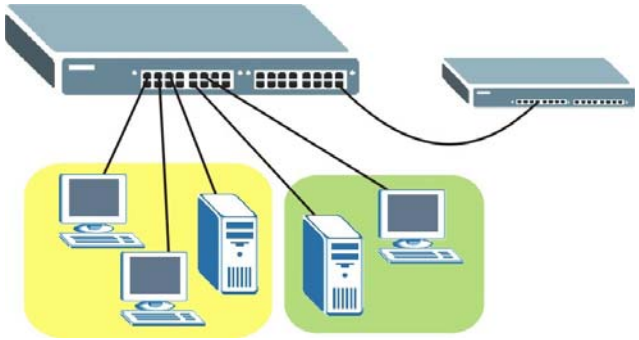
LABEL	DESCRIPTION
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.6 Protocol Based VLANs

Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the Switch checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed in the same protocol based VLAN. One advantage of using protocol based VLANs is that priority can be assigned to traffic of the same protocol.

For example, port 1, 2, 3 and 4 belong to static VLAN 100, and port 4, 5, 6, 7 belong to static VLAN 120. You configure a protocol based VLAN A with priority 3 for ARP traffic received on port 1, 2 and 3. You also have a protocol based VLAN B with priority 2 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic, when they go through the uplink port to a backbone switch C.

Figure 57 Protocol Based VLAN Application Example



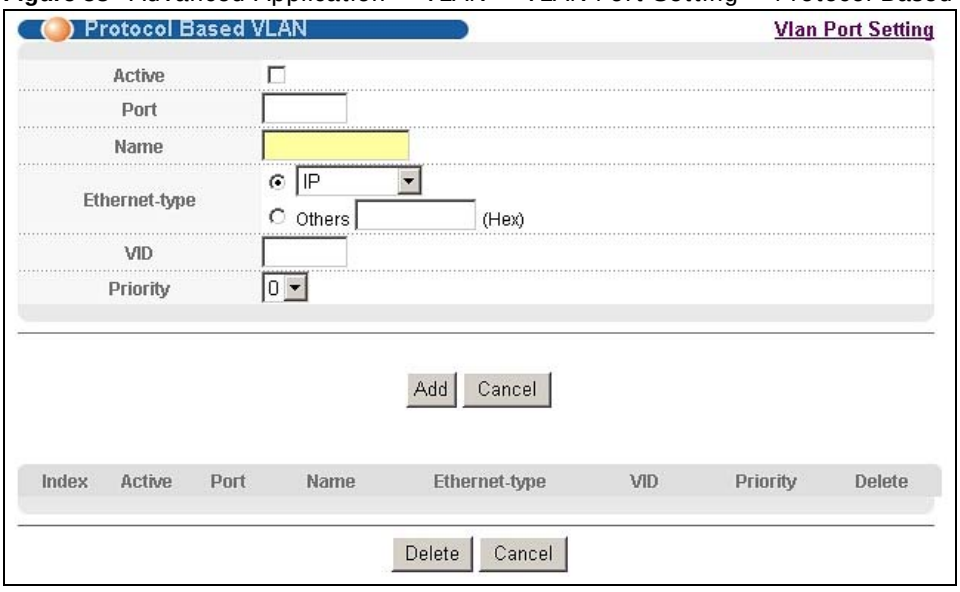
9.6.1 Configuring Protocol Based VLAN

Click **Protocol Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Note: Protocol-based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

Note: You can not enable protocol-based VLANs on the Switch when the Guest VLAN feature is activated on a port.

Figure 58 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN



The following table describes the labels in this screen.

Table 22 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this protocol based VLAN.
Port	Type a port to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN. See Chapter 9 on page 83 for more details on setting up VLANs.
Name	Enter up to 32 alpha numeric characters to identify this protocol based VLAN.
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select **Others** and type the protocol number in hexadecimal notation. For example the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137. Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VID	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the **Advanced Applications** > **VLAN** screens.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the index number identifying this protocol based VLAN. Click on any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.

Table 22 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Name	This field shows the name the protocol based VLAN.
Ethernet Type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.7 Port-based VLAN Setup

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the Switch on which they were created.

Note: When you activate port-based VLAN, the Switch uses a default VLAN ID of 1. You cannot change it.

Note: In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

9.7.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Basic Setting** > **Switch Setup** screen and then click **Advanced Application** > **VLAN** from the navigation panel to display the next screen.

Figure 59 Port Based VLAN Setup (All Connected)

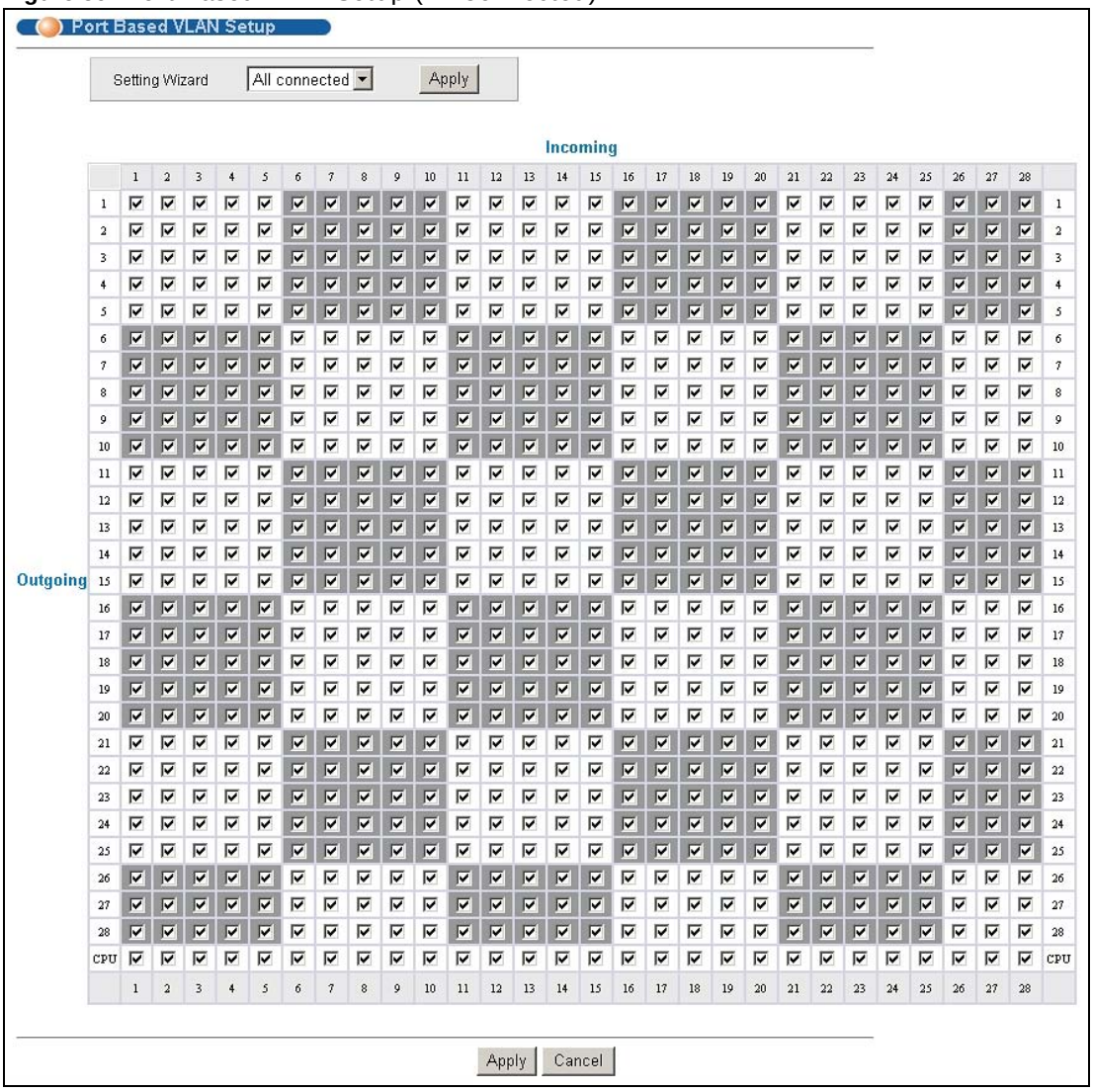
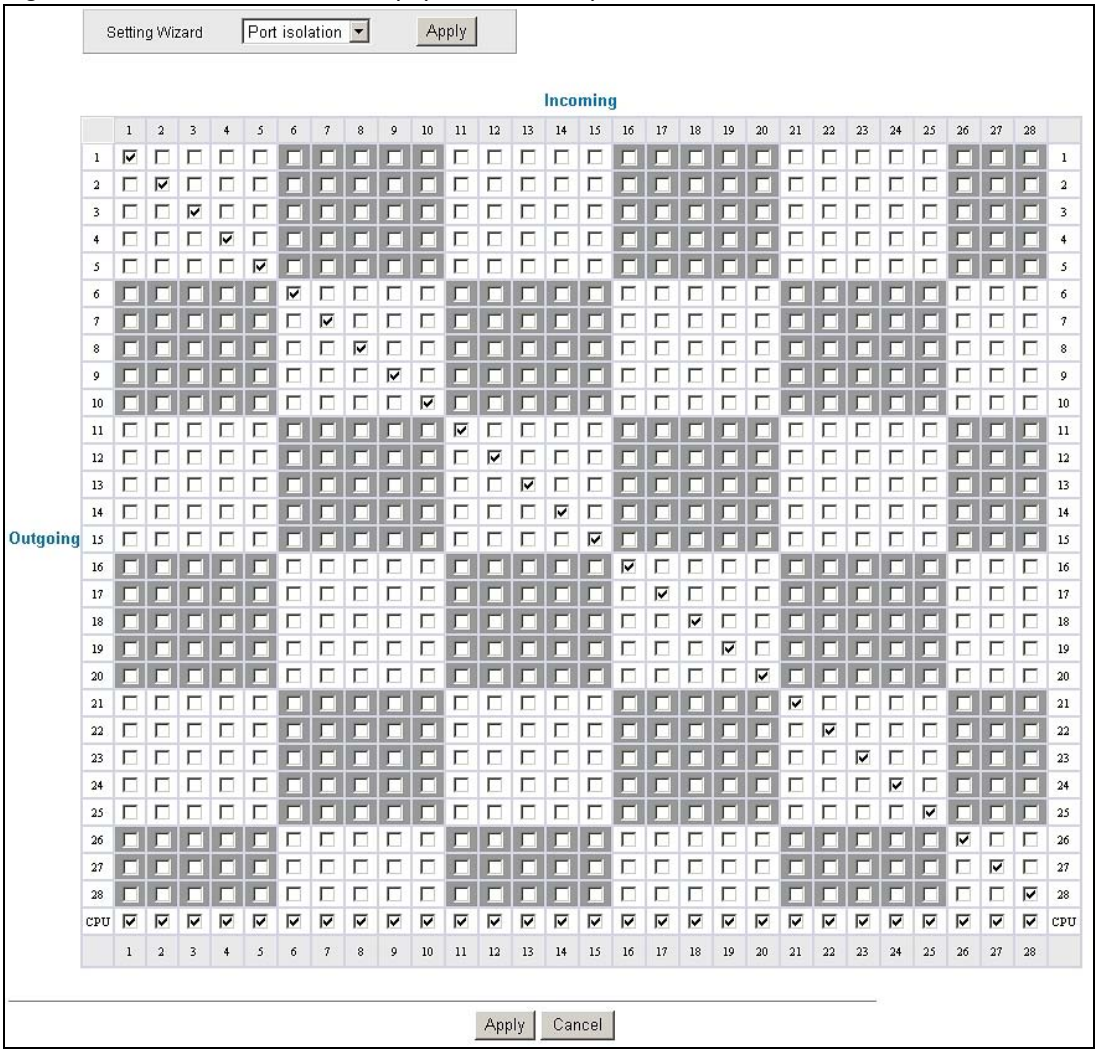


Figure 60 Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 23 Port Based VLAN Setup

label	Description
Setting Wizard	Choose **All connected** or **Port isolation**. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure. After you make your selection, click **Apply** (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click **Apply** at the bottom of the screen.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.8 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

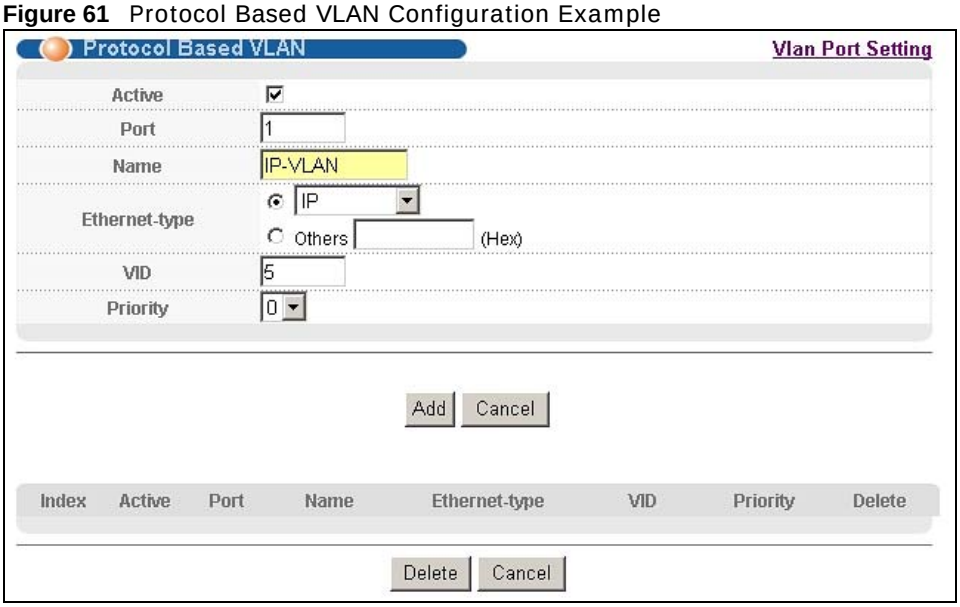
9.8.1 Create an IP-based VLAN Example

This example shows you how to create an IP VLAN which includes ports 1, 4 and 8. Follow these steps:

1. Activate this protocol based VLAN.
2. Type the port number you want to include in this protocol based VLAN. Type **1**.
3. Give this protocol-based VLAN a descriptive name. Type **IP-VLAN**.
4. Select the protocol. Leave the default value **IP**.
5. Type the VLAN ID of an existing VLAN. In our example we already created a static VLAN with an ID of 5. Type **5**.

6 Leave the priority set to **0** and click **Add**.

Figure 61 Protocol Based VLAN Configuration Example



To add more ports to this protocol based VLAN.

1 Click the index number of the protocol based VLAN entry. Click **1**

2 Change the value in the **Port** field to the next port you want to add.

3 Click **Add**.

10

Static MAC Forward Setup

10.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

Use these screens to configure static MAC address forwarding.

10.1.1 What You Can Do

Use the **Static MAC Forwarding** screen (Section 10.2 on page 101) to assign static MAC addresses for a port.

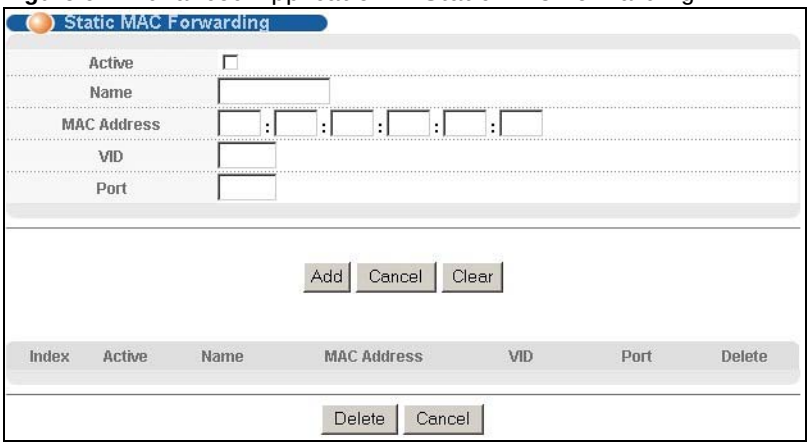
10.2 Configuring Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch. See Chapter 19 on page 151 for more information on port security.

Click **Advanced Application** > **Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 62 Advanced Application > Static MAC Forwarding



The following table describes the labels in this screen.

Table 24 Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click **Add** to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

11

Static Multicast Forward Setup

11.1 Overview

This chapter discusses how to configure forwarding rules based on multicast MAC addresses of devices on your network.

Use these screens to configure static multicast address forwarding.

11.1.1 What You Can Do

Use the **Static Multicast Forward Setup** screen (Section 11.2 on page 104) to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

11.1.2 What You Need To Know

A multicast MAC address is the MAC address of a member of a multicast group. A static multicast address is a multicast MAC address that has been manually entered in the multicast table. Static multicast addresses do not age out. Static multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. You can configure this in the **Advanced Application** > **Multicast** > **Multicast Setting** screen (see Section 23.3 on page 171). Figure 63 shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s)

within a VLAN group. Figure 64 shows frames being forwarded to devices connected to port 3. Figure 65 shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 63 No Static Multicast Forwarding

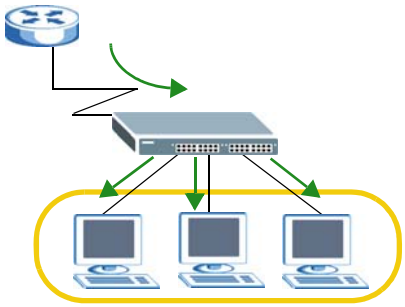


Figure 64 Static Multicast Forwarding to A Single Port

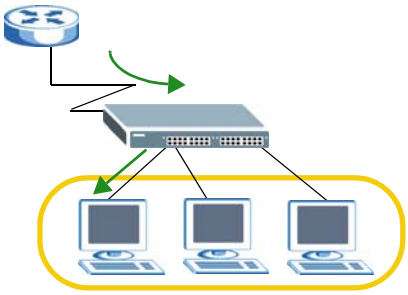
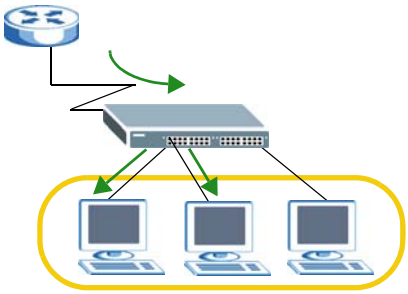


Figure 65 Static Multicast Forwarding to Multiple Ports

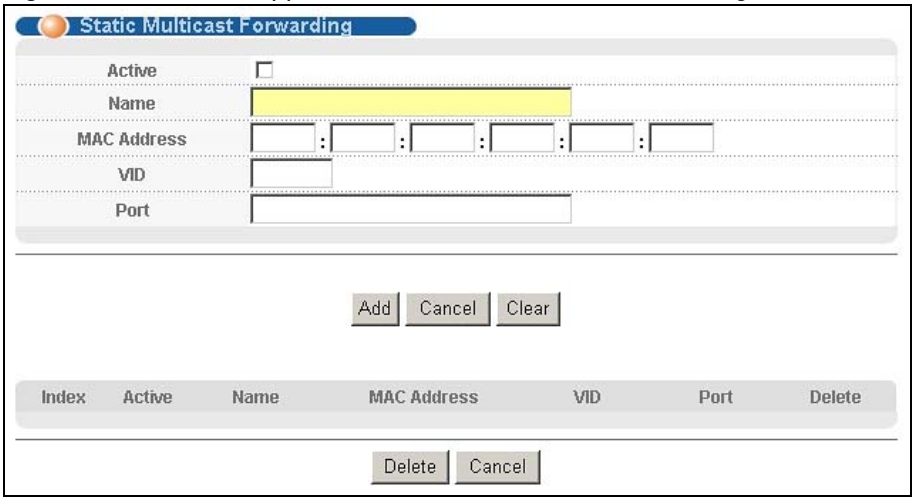


11.2 Configuring Static Multicast Forwarding

Use this screen to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

Click **Advanced Application** > **Static Multicast Forwarding** to display the configuration screen as shown.

Figure 66 Advanced Application > Static Multicast Forwarding



The following table describes the labels in this screen.

Table 25 Advanced Application > Static Multicast Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don't have a specific target VLAN, enter 1.
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Add	Click **Add** to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to begin configuring this screen afresh.
Index	Click an index number to modify a static multicast MAC address rule for port(s).
Active	This field displays whether a static multicast MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.

Table 25 Advanced Application > Static Multicast Forwarding (continued)

LABEL	DESCRIPTION
Port	This field displays the port(s) within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

12 Filtering

12.1 Overview

This chapter discusses MAC address port filtering.

Filtering means sifting traffic going through the Switch based on the source and/or destination MAC addresses and VLAN group (ID).

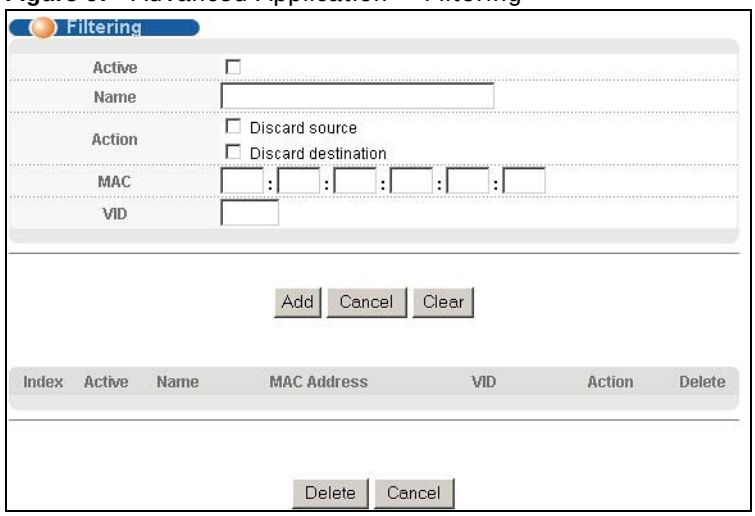
12.1.1 What You Can Do

Use the **Filtering** screen (Section 12.2 on page 107) to create rules for traffic going through the Switch.

12.2 Configure a Filtering Rule

Use this screen to create rules for traffic going through the Switch. Click **Advanced Application** > **Filtering** in the navigation panel to display the screen as shown next.

Figure 67 Advanced Application > Filtering



The following table describes the related labels in this screen.

Table 26 Advanced Application > Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.
Action	Select **Discard source** to drop the frames from the source MAC address (specified in the **MAC** field). The Switch can still send frames to the MAC address. Select **Discard destination** to drop the frames to the destination MAC address (specified in the **MAC** address). The Switch can still receive frames originating from the MAC address. Select **Discard source** and **Discard destination** to block traffic to/from the MAC address specified in the **MAC** field.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Action	This field displays the filter type for the MAC address.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

13

Spanning Tree Protocol

13.1 Overview

The Switch supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

13.1.1 What You Can Do

- Use the **Spanning Tree Protocol** status screen (Section 13.2 on page 112) to view the STP status in the different STP modes (RSTP, MRSTP or MSTP) you can configure on the Switch.
- Use the **Spanning Tree Configuration** screen (Section 13.3 on page 113) to activate one of the STP modes on the Switch.
- Use the **Rapid Spanning Tree Protocol** screen (Section 13.4 on page 114) to configure RSTP settings.
- Use the **Rapid Spanning Tree Protocol Status** screen (Section 13.5 on page 115) to display the status screen as shown next.
- Use the **Multiple Rapid Spanning Tree Protocol** screen (Section 13.6 on page 117) to configure MRSTP.
- Use the **Multiple Rapid Spanning Tree Protocol Status** screen (Section 13.7 on page 118) to view the MRSTP status.
- Use the **Multiple Spanning Tree Protocol** screen (Section 13.8 on page 120) to configure MSTP.
- Use the **MSTP Port Configuration** screen (Section 13.8.1 on page 123) to configure MSTP ports.
- Use the **Multiple Spanning Tree Protocol Status** screen (Section 13.9 on page 123) to view the MSTP status.

13.1.2 What You Need to Know

Read on for concepts on STP that can help you configure the screens in this chapter.

(Rapid) Spanning Tree Protocol

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 27 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a

predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 28 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

Multiple RSTP

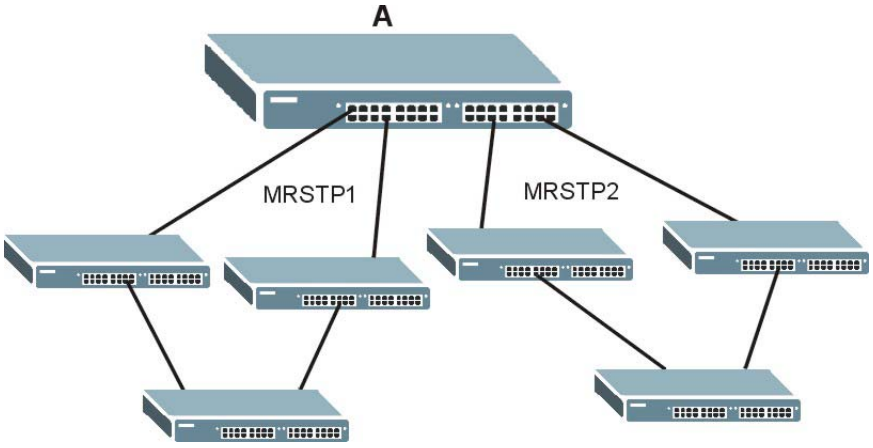
MRSTP (Multiple RSTP) is ZyXEL's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign port(s) to each tree. Each spanning tree operates independently with its own bridge information.

In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

To set up MRSTP, activate MRSTP on the Switch and specify which port(s) belong to which spanning tree.

Note: Each port can belong to one STP tree only.

Figure 68 MRSTP Network Example



Multiple STP

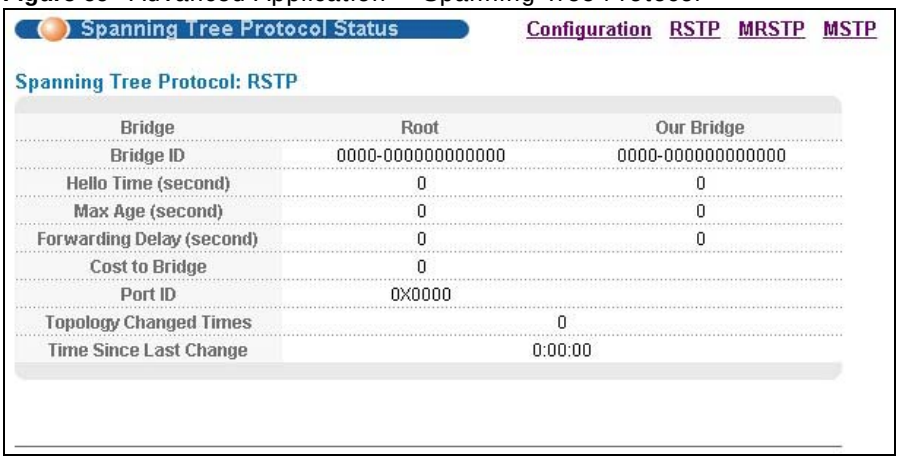
Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

13.2 Spanning Tree Protocol Status Screen

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **Advanced Application** > **Spanning Tree Protocol** to see the screen as shown.

Figure 69 Advanced Application > Spanning Tree Protocol



This screen differs depending on which STP mode (RSTP, MRSTP or MSTP) you configure on the Switch. This screen is described in detail in the section that follows the configuration section for each STP mode. Click **Configuration** to activate one of the STP standards on the Switch.

13.3 Spanning Tree Configuration

Use the **Spanning Tree Configuration** screen to activate one of the STP modes on the Switch. Click **Configuration** in the **Advanced Application** > **Spanning Tree Protocol**.

Figure 70 Advanced Application > Spanning Tree Protocol > Configuration

The following table describes the labels in this screen.

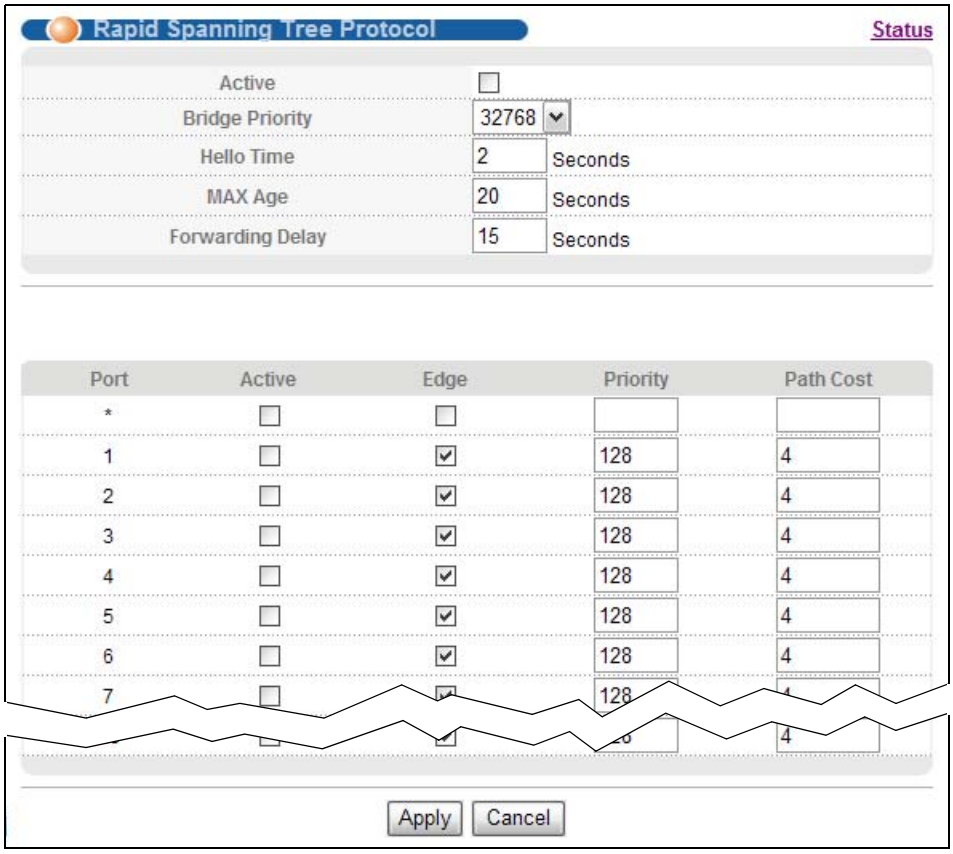
Table 29 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select **Rapid Spanning Tree**, **Multiple Rapid Spanning Tree** or **Multiple Spanning Tree**. See Section 13.1 on page 109 for background information on STP.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see (Rapid) Spanning Tree Protocol on page 110 for more information on RSTP. Click **RSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen.

Figure 71 Advanced Application > Spanning Tree Protocol > RSTP



The following table describes the labels in this screen.

Table 30 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **RSTP Status** screen (see Figure 72 on page 116).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP. Note: You must also activate **Rapid Spanning Tree** in the **Advanced Application > Spanning Tree Protocol > Configuration** screen to enable RSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.

Table 30 Advanced Application > Spanning Tree Protocol > RSTP (continued)

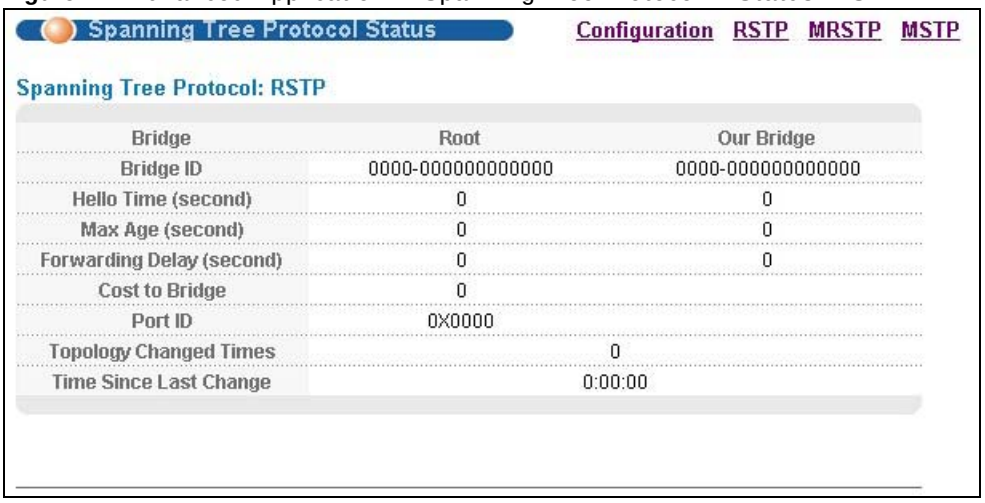
LABEL	DESCRIPTION
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 27 on page 110 for more information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 13.1 on page 109 for more information on RSTP.

Note: This screen is only available after you activate RSTP on the Switch.

Figure 72 Advanced Application > Spanning Tree Protocol > Status: RSTP



The following table describes the labels in this screen.

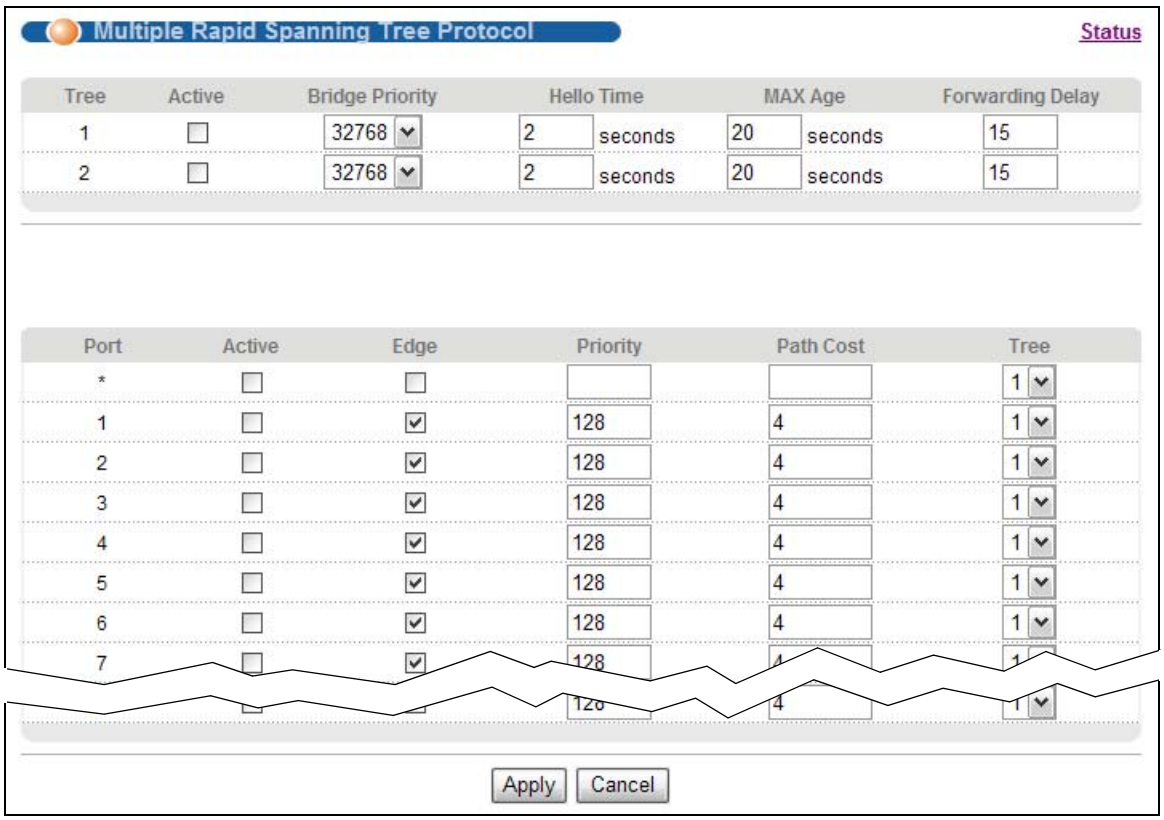
Table 31 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **RSTP** to edit RSTP settings on the Switch.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

13.6 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Multiple RSTP on page 111 for more information on MRSTP.

Figure 73 Advanced Application > Spanning Tree Protocol > MRSTP



The following table describes the labels in this screen.

Table 32 Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MRSTP Status** screen (see Figure 72 on page 116).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree. Note: You must also activate **Multiple Rapid Spanning Tree** in the **Advanced Application** > **Spanning Tree Protocol** > **Configuration** screen to enable MRSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.

Table 32 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

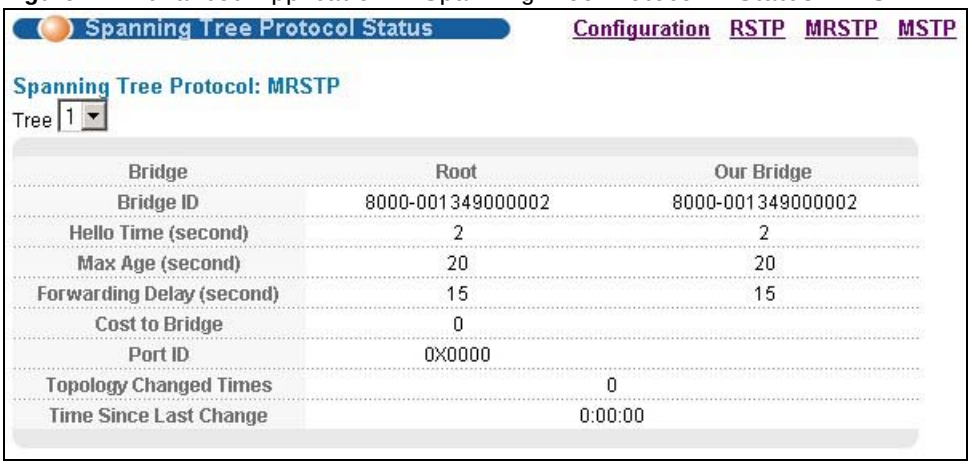
LABEL	DESCRIPTION
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate STP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 27 on page 110 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.7 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 13.1 on page 109 for more information on MRSTP.

Note: This screen is only available after you activate MRSTP on the Switch.

Figure 74 Advanced Application > Spanning Tree Protocol > Status: MRSTP



The following table describes the labels in this screen.

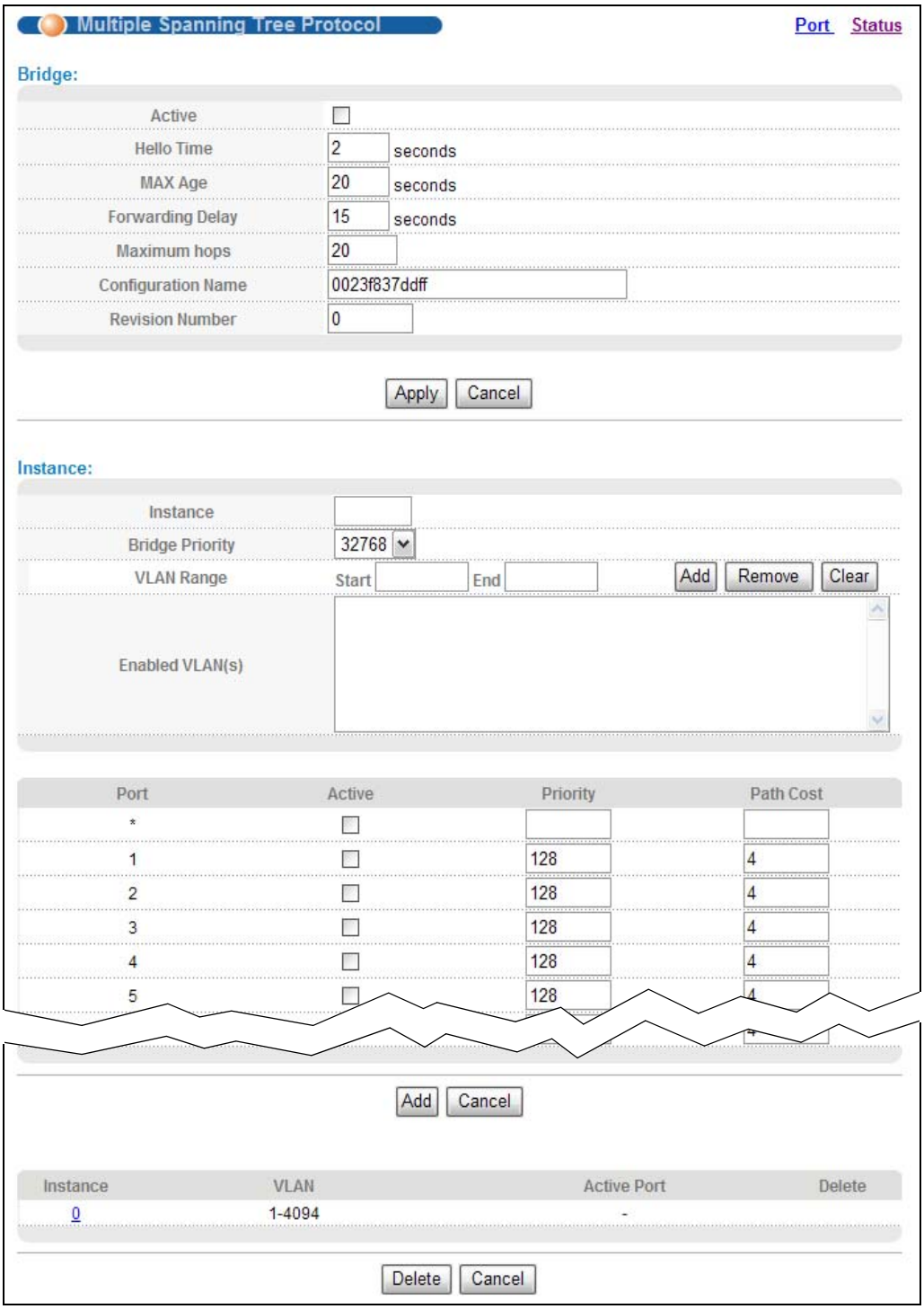
Table 33 Advanced Application > Spanning Tree Protocol > Status: MRSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MRSTP** to edit MRSTP settings on the Switch.
Tree	Select which STP tree configuration you want to view.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

13.8 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Multiple STP on page 112 for more information on MSTP.

Figure 75 Advanced Application > Spanning Tree Protocol > MSTP



The following table describes the labels in this screen.

Table 34 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MSTP Status** screen (see Figure 77 on page 124).
Port	Click **Port** to display the **MSTP Port Configuration** screen (see Figure 76 on page 123).
Active	Select this to activate MSTP on the Switch. Clear this to disable MSTP on the Switch. Note: You must also activate **Multiple Spanning Tree** in the **Advanced Application > Spanning Tree Protocol > Configuration** screen to enable MSTP on the Switch.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MaxAge	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0-15.
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).

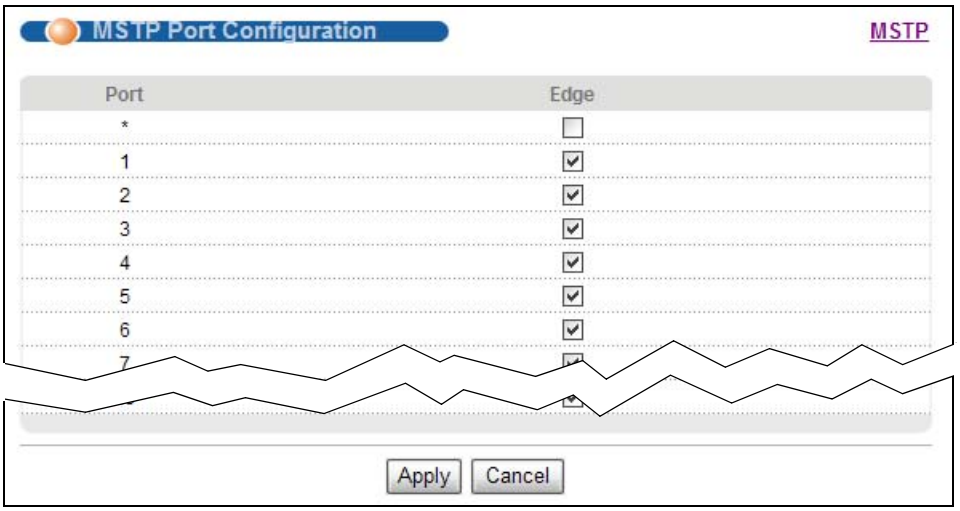
Table 34 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **Start** field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **End** field. Next click: • **Add** - to add this range of VLAN(s) to be mapped to the MST instance. • **Remove** - to remove this range of VLAN(s) from being mapped to the MST instance. • **Clear** - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 27 on page 110 for more information.
Add	Click **Add** to save this MST instance to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.8.1 Multiple Spanning Tree Protocol Port Configuration

To configure MSTP ports, click **Port** in the **Advanced Application** > **Spanning Tree Protocol** > **MSTP** screen.

Figure 76 Advanced Application > Spanning Tree Protocol > MSTP > Port



The following table describes the labels in this screen.

Table 35 Advanced Application > Spanning Tree Protocol > MSTP > Port

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.9 Multiple Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Multiple STP on page 112 for more information on MSTP.

Note: This screen is only available after you activate MSTP on the Switch.

Figure 77 Advanced Application > Spanning Tree Protocol > Status: MSTP

The following table describes the labels in this screen.

Table 36 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MSTP** to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.

Table 36 Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance:	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	**Root** refers to the base of the MST instance. **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.

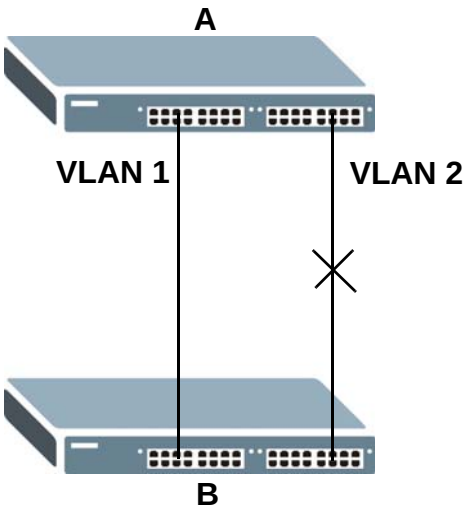
13.10 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

13.10.1 MSTP Network Example

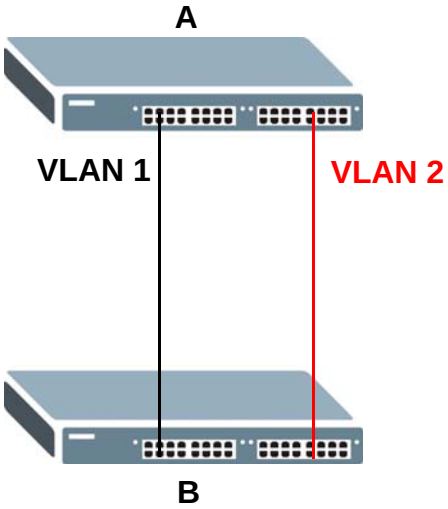
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 78 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 79 MSTP Network Example



13.10.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

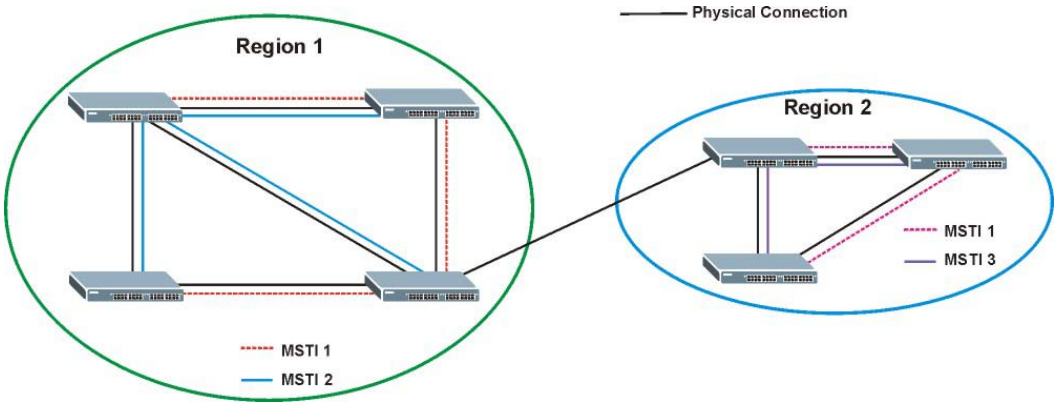
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

13.10.3 MST Instance

An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

Figure 80 MSTIs in Different Regions

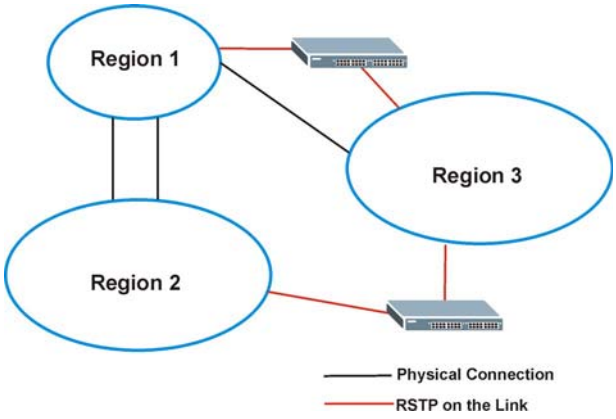


13.10.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST

that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

Figure 81 MSTP and Legacy RSTP Network Example



14

Bandwidth Control

14.1 Overview

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

Bandwidth control means defining a maximum allowable bandwidth for out-going traffic flows on a port.

14.1.1 What You Can Do

Use the **Bandwidth Control** screen (Section 14.2 on page 130) to limit the bandwidth for traffic going through the Switch.

14.2 Bandwidth Control Setup

Click **Advanced Application** > **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 82 Advanced Application > Bandwidth Control

The following table describes the related labels in this screen.

Table 37 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate ingress rate limits on this port.
Ingress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. Note: Ingress rate bandwidth control applies to layer 2 traffic only.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.

Table 37 Advanced Application > Bandwidth Control (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

15

Broadcast Storm Control

15.1 Overview

This chapter introduces and shows you how to configure the broadcast storm control feature.

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

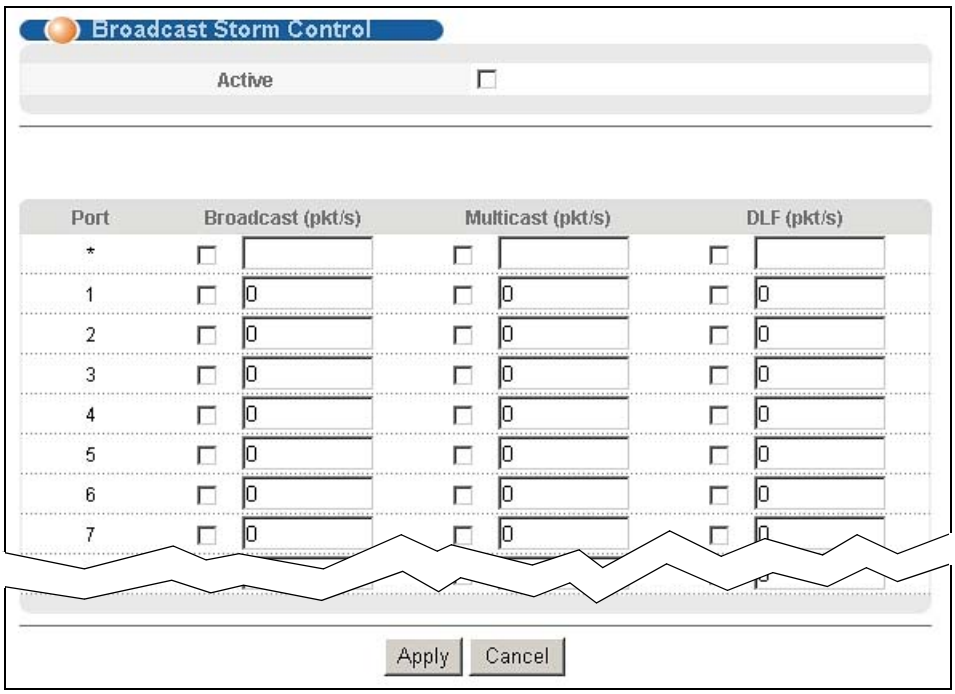
15.1.1 What You Can Do

Use the **Broadcast Storm Control** screen (Section 15.2 on page 133) to limit the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.

15.2 Broadcast Storm Control Setup

Click **Advanced Application** > **Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 83 Advanced Application > Broadcast Storm Control



The following table describes the labels in this screen.

Table 38 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

16

Mirroring

16.1 Overview

This chapter discusses port mirroring setup screens.

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

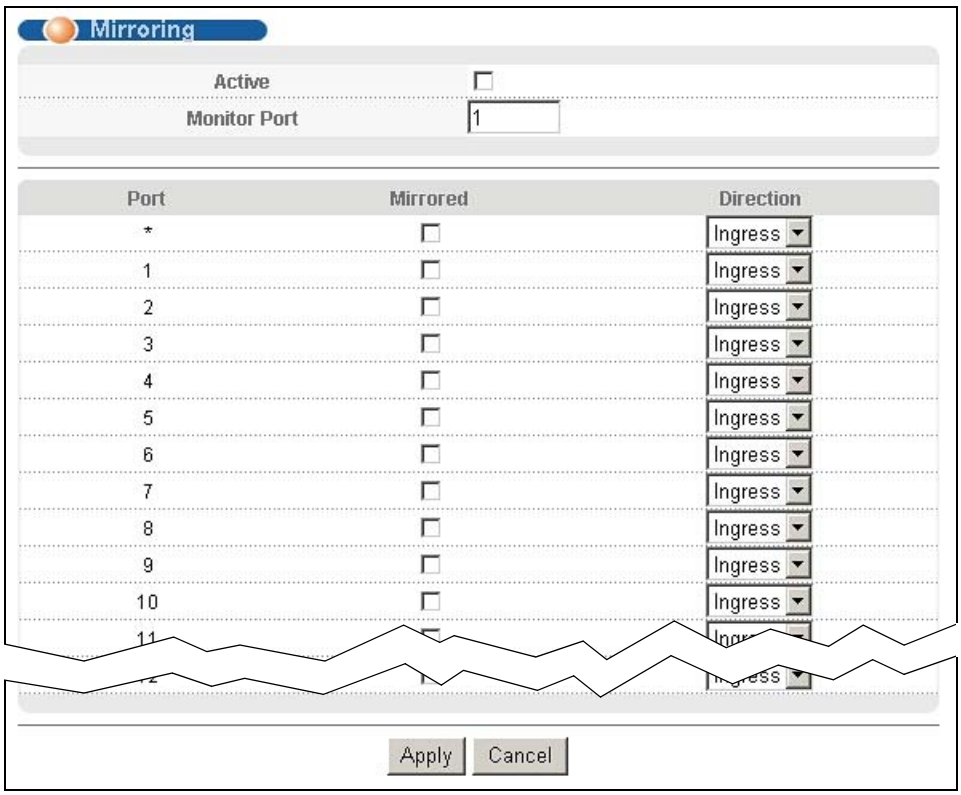
16.1.1 What You Can Do

Use the **Mirroring** screen (Section 16.2 on page 135) to select a monitor port and specify the traffic flow to be copied to the monitor port.

16.2 Port Mirroring Setup

Click **Advanced Application > Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 84 Advanced Application > Mirroring



The following table describes the labels in this screen.

Table 39 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Enter the port number of the monitor port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are **Egress** (outgoing), **Ingress** (incoming) and **Both**.

Table 39 Advanced Application > Mirroring (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

17

Link Aggregation

17.1 Overview

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link. However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

17.1.1 What You Can Do

- Use the **Link Aggregation Status** screen (Section 17.2 on page 138) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen (Section 17.3 on page 140) to configure to enable static link aggregation.
- Use the **Link Aggregation Control Protocol** screen (Section 17.4 on page 142) to enable Link Aggregation Control Protocol (LACP).

17.1.2 What You Need to Know

The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

See Section 17.5.1 on page 143 for a static port trunking example.

Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that

is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

Link Aggregation ID

LACP aggregation ID consists of the following information[1]:

Table 40 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

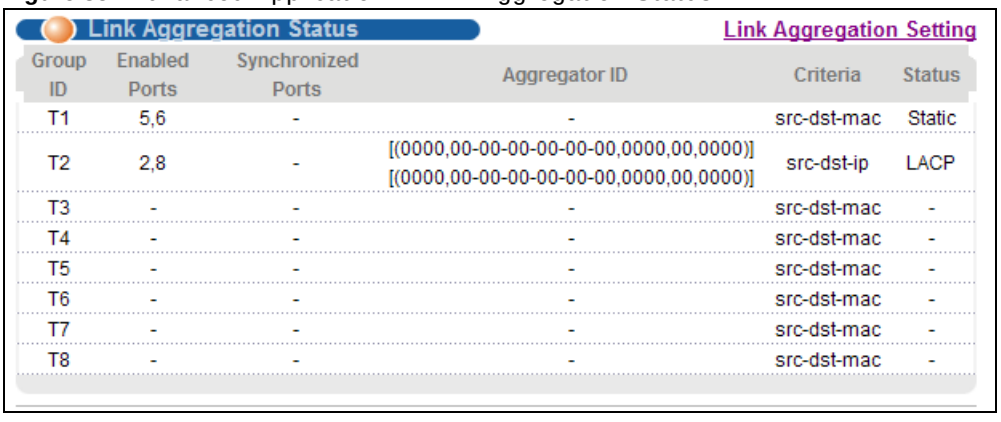
Table 41 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

17.2 Link Aggregation Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See Section 17.1 on page 137 for more information.

Figure 85 Advanced Application > Link Aggregation Status


Link Aggregation Status

Link Aggregation Setting

Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
T1	5,6	-	-	src-dst-mac	Static
T2	2,8	-	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	src-dst-ip	LACP
T3	-	-	-	src-dst-mac	-
T4	-	-	-	src-dst-mac	-
T5	-	-	-	src-dst-mac	-
T6	-	-	-	src-dst-mac	-
T7	-	-	-	src-dst-mac	-
T8	-	-	-	src-dst-mac	-

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

The following table describes the labels in this screen.

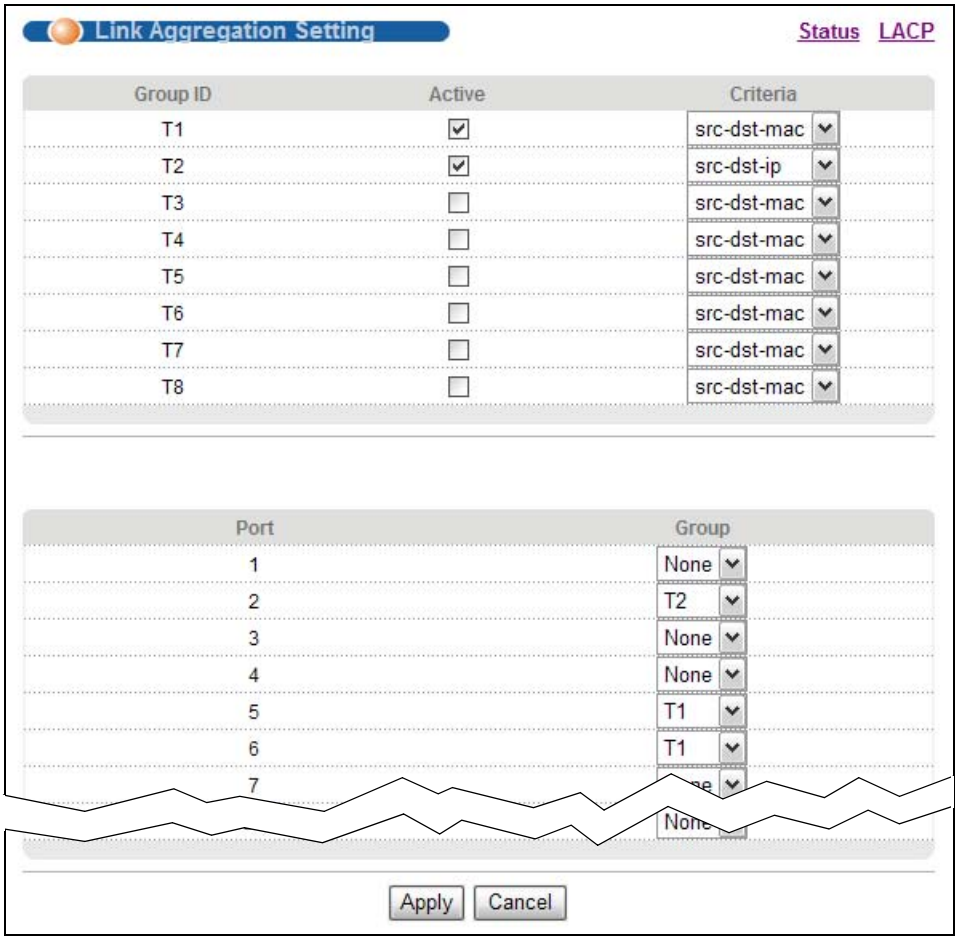
Table 42 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group. The port number(s) displays only when this trunk group is activated and there is a port belonging to this group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Link Aggregation ID on page 138 for more information on this field. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. **src-mac** means the Switch distributes traffic based on the packet's source MAC address. **dst-mac** means the Switch distributes traffic based on the packet's destination MAC address. **src-dst-mac** means the Switch distributes traffic based on a combination of the packet's source and destination MAC addresses. **src-ip** means the Switch distributes traffic based on the packet's source IP address. **dst-ip** means the Switch distributes traffic based on the packet's destination IP address. **src-dst-ip** means the Switch distributes traffic based on a combination of the packet's source and destination IP addresses.
Status	This field displays how these ports were added to the trunk group. It displays: • **Static** - if the ports are configured as static members of a trunk group. • **LACP** - if the ports are configured to join a trunk group via LACP.

17.3 Link Aggregation Setting

Click **Advanced Application** > **Link Aggregation > Link Aggregation Setting** to display the screen shown next. See Section 17.1 on page 137 for more information on link aggregation.

Figure 86 Advanced Application > Link Aggregation > Link Aggregation Setting



The following table describes the labels in this screen.

Table 43 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.

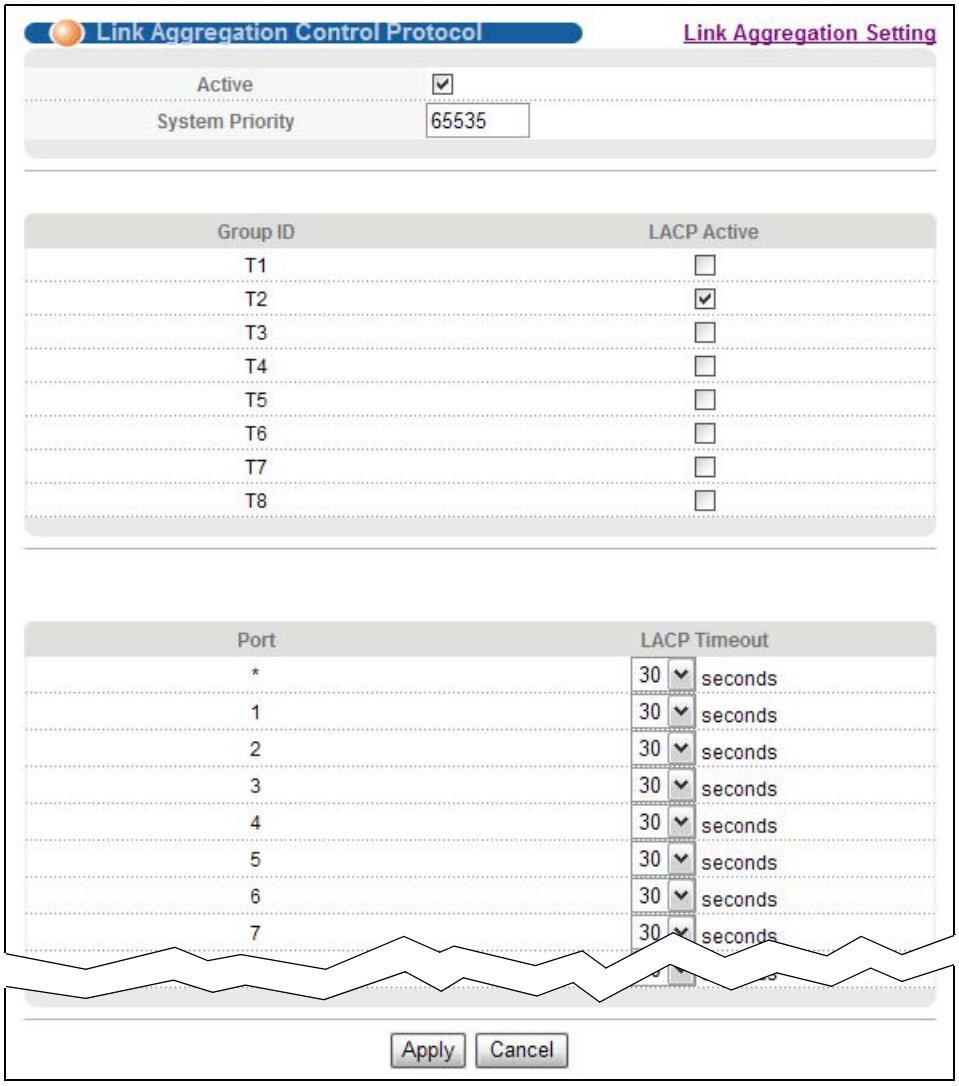
Table 43 Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

LABEL	DESCRIPTION
Criteria	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the **src-dst-mac** distribution type. If the Switch is behind a router, the packet's destination or source MAC address will be changed. In this case, set the Switch to distribute traffic based on its IP address to make sure port trunking can work properly. Select **src-mac** to distribute traffic based on the packet's source MAC address. Select **dst-mac** to distribute traffic based on the packet's destination MAC address. Select **src-dst-mac** to distribute traffic based on a combination of the packet's source and destination MAC addresses. Select **src-ip** to distribute traffic based on the packet's source IP address. Select **dst-ip** to distribute traffic based on the packet's destination IP address. Select **src-dst-ip** to distribute traffic based on a combination of the packet's source and destination IP addresses.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs. Note: When you enable the port security feature on the Switch and configure port security settings for a port, you cannot include the port in an active trunk group.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.4 Link Aggregation Control Protocol

Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** > **LACP** to display the screen shown next. See Dynamic Link Aggregation on page 137 for more information on dynamic link aggregation.

Figure 87 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



The following table describes the labels in this screen.

Table 44 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).

Table 44 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (continued)

LABEL	DESCRIPTION
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be "down" and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.5 Technical Reference

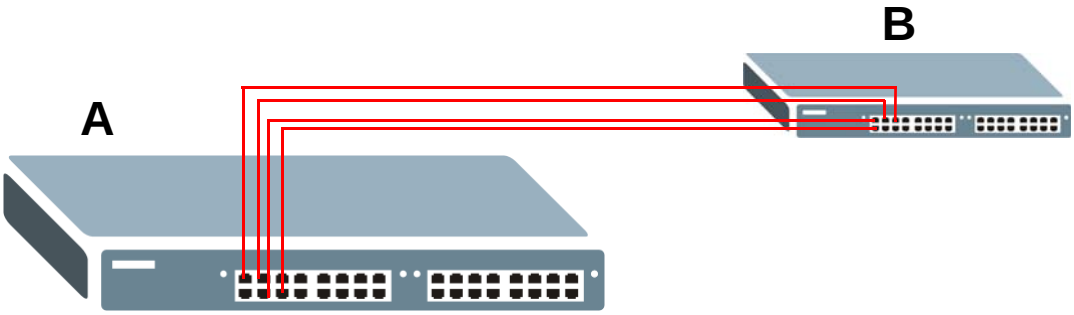
This section provides technical background information on the topics discussed in this chapter.

17.5.1 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

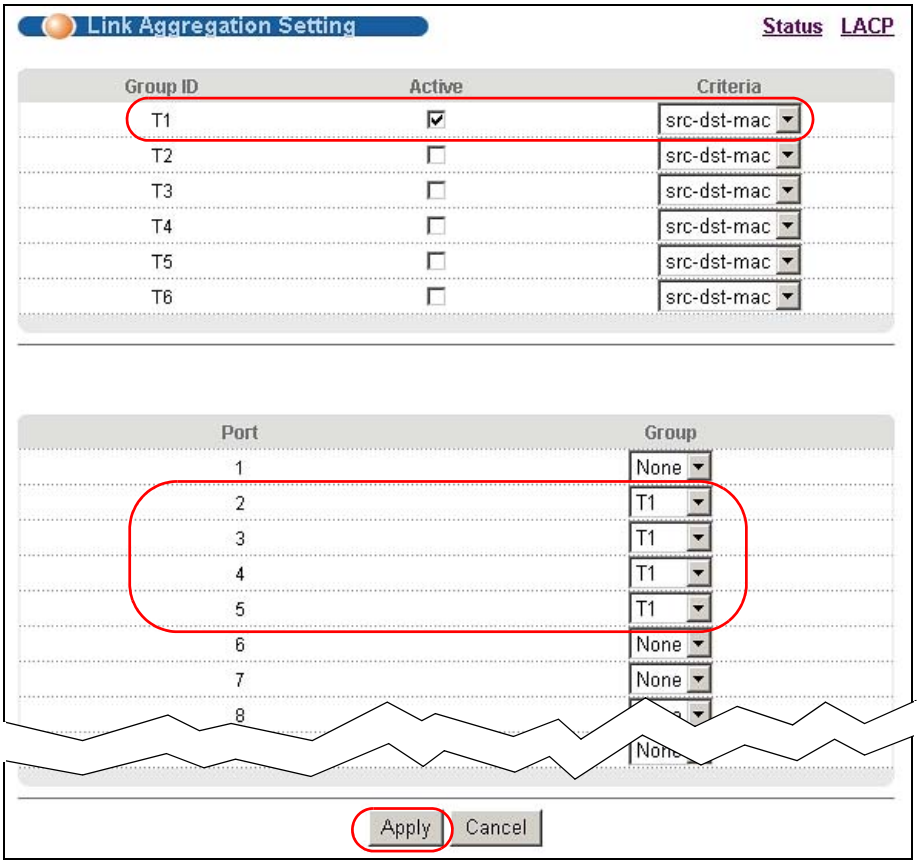
1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

Figure 88 Trunking Example - Physical Connections



2 **Configure static trunking** - Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting**. In this screen activate trunk group **T1**, select the traffic distribution algorithm used by this group and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

Figure 89 Trunking Example - Configuration Screen



Your trunk group 1 (**T1**) configuration is now complete.

18

Port Authentication

18.1 Overview

This chapter describes the IEEE 802.1x authentication method.

Port authentication is a way to validate access to ports on the Switch to clients based on an external server (authentication server). The Switch supports the following method for port authentication:

- **IEEE 802.1x**[2] - An authentication server validates access to a port based on a username and password provided by the user.

18.1.1 What You Can Do

- Use the **Port Authentication** screen (Section 18.2 on page 146) to check if IEEE 802.1x port authentication is activated.
- Use the **802.1x** screen (Section 18.3 on page 147) to activate IEEE 802.1x security.
- Use the **Guest VLAN** screen (Section 18.3 on page 147) to activate IEEE 802.1x security.

18.1.2 What You Need to Know

IEEE 802.1x authentication uses the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See RADIUS and TACACS+ on page 183 for more information on configuring your RADIUS server settings.

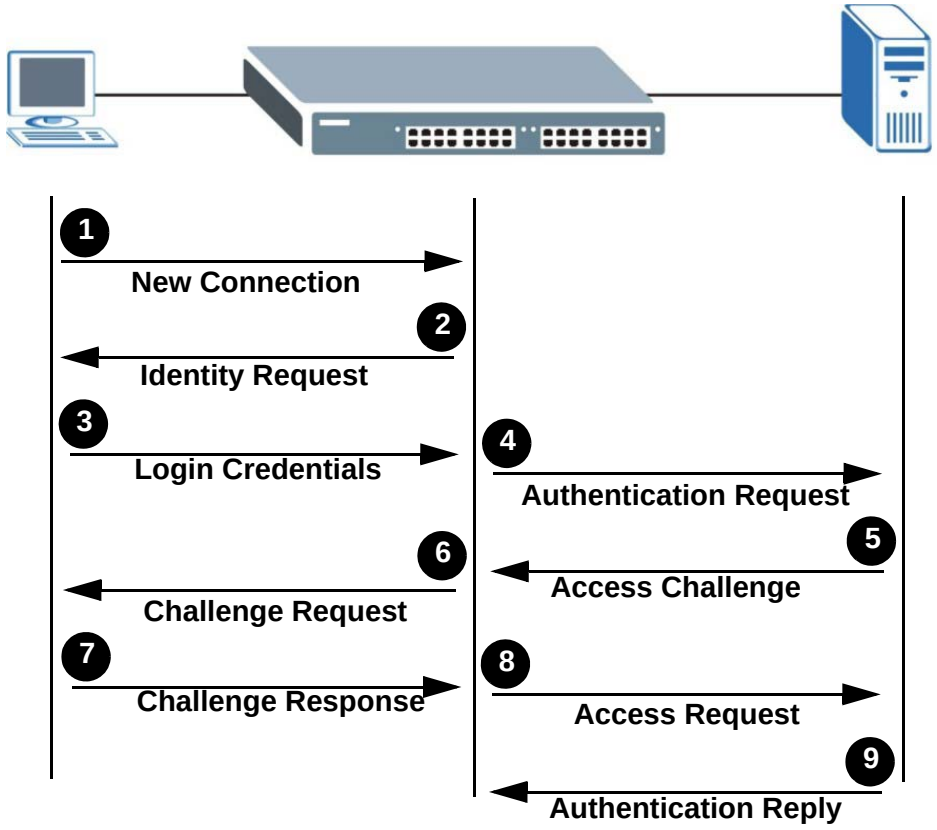
IEEE 802.1x Authentication

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the Switch sends an

2. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Figure 90 IEEE 802.1x Authentication Process



18.2 Port Authentication Configuration

To enable port authentication, first activate the port authentication method (both on the Switch and the port(s)) then configure the RADIUS server settings in the **Auth and Acct > Radius Server Setup** screen.

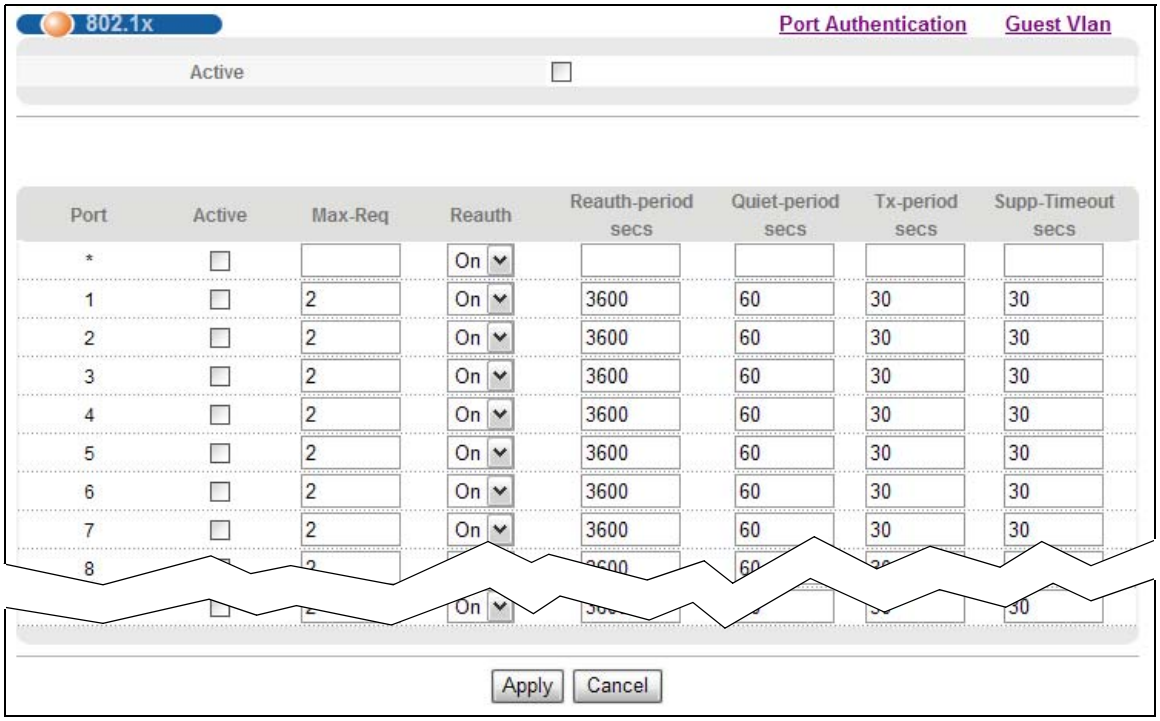
Click **Advanced Application** > **Port Authentication** in the navigation panel to display the screen as shown.

Figure 91 Advanced Application > Port Authentication

18.3 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. In the **Port Authentication** screen click **802.1x** to display the configuration screen as shown.

Figure 92 Advanced Application > Port Authentication > 802.1x



The following table describes the labels in this screen.

Table 45 Advanced Application > Port Authentication > 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Max-Req	Specify the number of times the Switch tries to authenticate client(s) before sending unresponsive ports to the Guest VLAN. This is set to 2 by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch blocks the client from accessing the port or sends the client to the Guest VLAN when a Guest VLAN is enabled on the port. The client needs to send a new request to be authenticated by the Switch again.

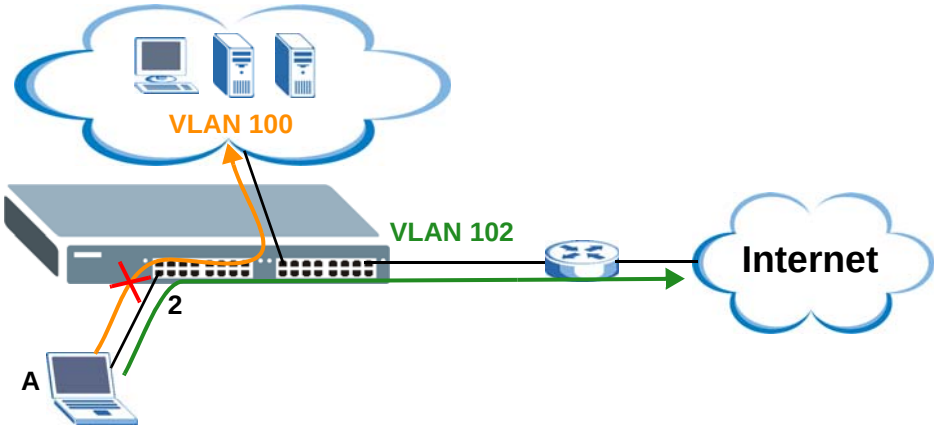
Table 45 Advanced Application > Port Authentication > 802.1x (continued)

LABEL	DESCRIPTION
Reauth	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-period	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Quiet-period	Specify the number of seconds the port remains in the HELD state and rejects further authentication requests from the connected client after a failed authentication exchange.
Tx-period	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout	Specify the number of seconds the Switch waits for client's response to a challenge request before sending another request.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.3.1 Guest VLAN

When 802.1x port authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the port(s). You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (**102** in the example) on a port (**2** in the example), the user (**A** in the example) that is not IEEE 802.1x capable or fails to enter the correct username and password can still access the port, but traffic from the user is forwarded to the guest VLAN. That is, unauthenticated users can have access to limited network resources in the same guest VLAN, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

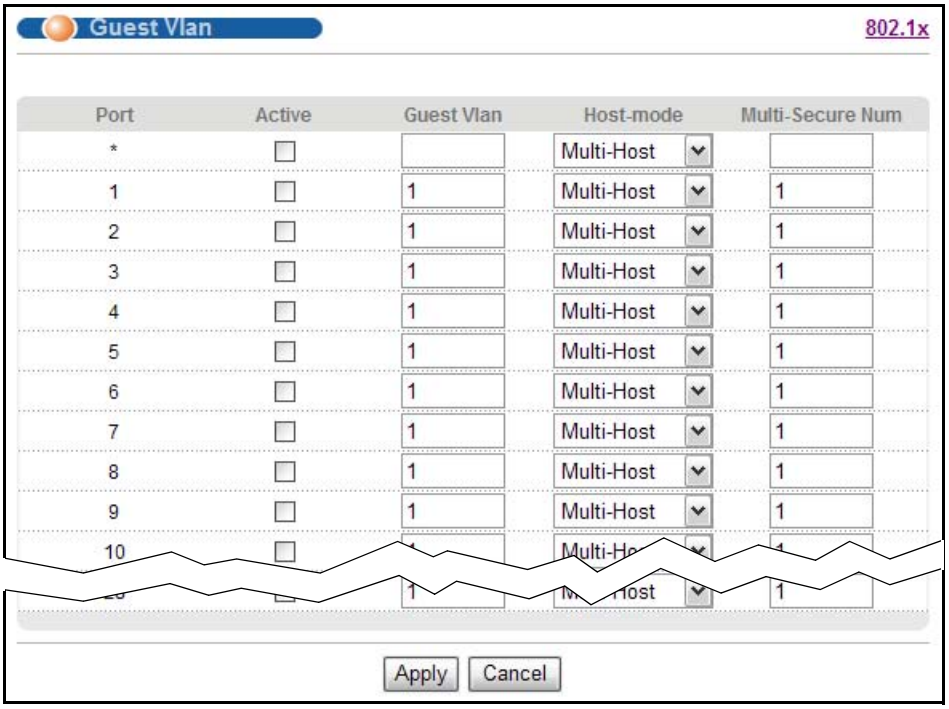
Figure 93 Guest VLAN Example



Use this screen to enable and assign a guest VLAN to a port. In the **Port Authentication > 802.1x** screen click **Guest Vlan** to display the configuration screen as shown.

Note: You can not enable the Guest VLAN feature on a port when a subnet-based VLAN or protocol-based VLAN is activated on the Switch.

Figure 94 Advanced Application > Port Authentication > 802.1x > Guest VLAN



The following table describes the labels in this screen.

Table 46 Advanced Application > Port Authentication > 802.1x > Guest VLAN

LABEL	DESCRIPTION
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the guest VLAN feature on this port. Clients that fail authentication are placed in the guest VLAN and can receive limited services.
Guest Vlan	A guest VLAN is a pre-configured VLAN on the Switch that allows non-authenticated users to access limited network resources through the Switch. You must also enable IEEE 802.1x authentication on the Switch and the associated ports. Enter the number that identifies the guest VLAN. Make sure this is a VLAN recognized in your network.
Host-mode	Specify how the Switch authenticates users when more than one user connect to the port (using a hub). Select **Multi-Host** to authenticate only the first user that connects to this port. If the first user enters the correct credential, any other users are allowed to access the port without authentication. If the first user fails to enter the correct credential, they are all put in the guest VLAN. Once the first user who did authentication logs out or disconnects from the port, rest of the users are blocked until a user does the authentication process again. Select **Multi-Secure** to authenticate each user that connects to this port.

Table 46 Advanced Application > Port Authentication > 802.1x > Guest VLAN (continued)

LABEL	DESCRIPTION
Multi-Secure Num	If you set **Host-mode** to **Multi-Secure**, specify the maximum number of users (between 1 and 9) that the Switch will authenticate on this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19

Port Security

19.1 Overview

This chapter shows you how to set up port security.

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

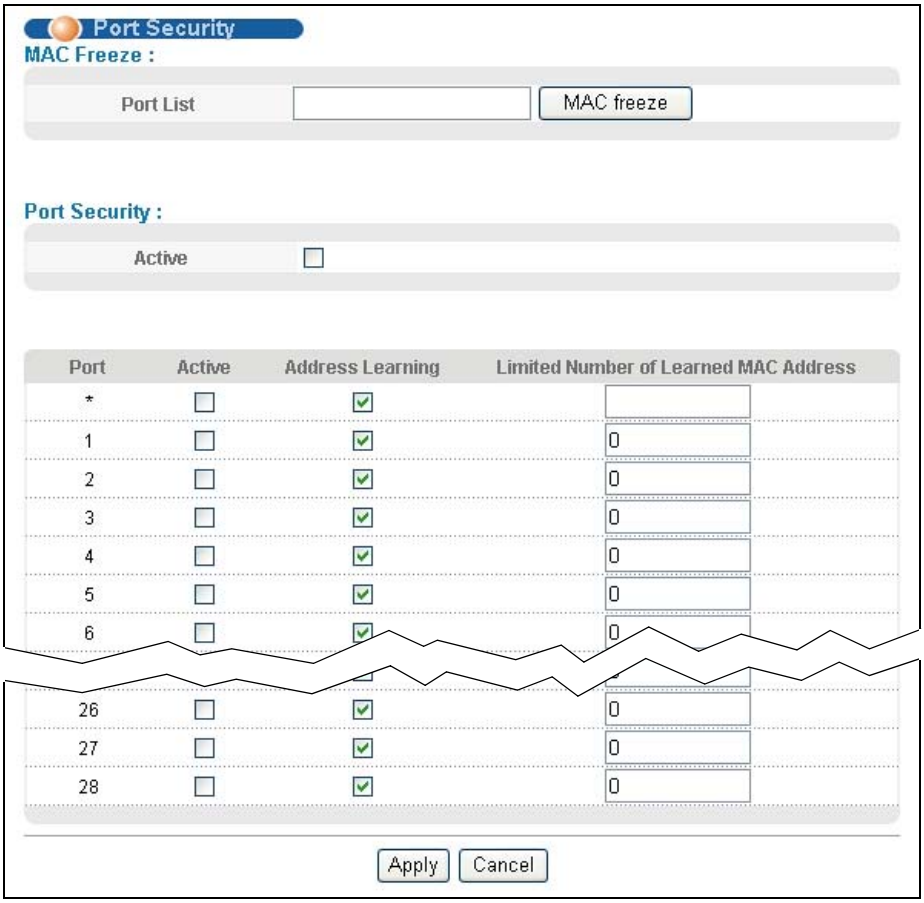
19.1.1 What You Can Do

Use the **Port Security** screen (Section 19.2 on page 152) to enable port security and disable MAC address learning. You can also enable the port security feature on a port.

19.2 Port Security Setup

Click **Advanced Application > Port Security** in the navigation panel to display the screen as shown.

Figure 95 Advanced Application > Port Security



The following table describes the labels in this screen.

Table 47 Advanced Application > Port Security

LABEL	DESCRIPTION
Port List	Enter the number of the port(s) (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click **MAC freeze**, all previously learned MAC addresses on the specified port(s) will become static MAC addresses and display in the **Static MAC Forwarding** screen.
MAC freeze	Click **MAC freeze** to have the Switch automatically select the **Active** check boxes and clear the **Address Learning** check boxes only for the ports specified in the **Port list**.
Active	Select this option to enable port security on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 47 Advanced Application > Port Security (continued)

LABEL	DESCRIPTION
Active	Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from “0” to “16384”. “0” means this feature is disabled.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20

Classifier

20.1 Overview

This chapter introduces and shows you how to configure the packet classifier on the Switch. It also discusses Quality of Service (QoS) and classifier concepts as employed by the Switch.

20.1.1 What You Can Do

Use the **Classifier** screen (Section 20.2 on page 154) to define the classifiers and view a summary of the classifier configuration. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.

20.1.2 What You Need to Know

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the Switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

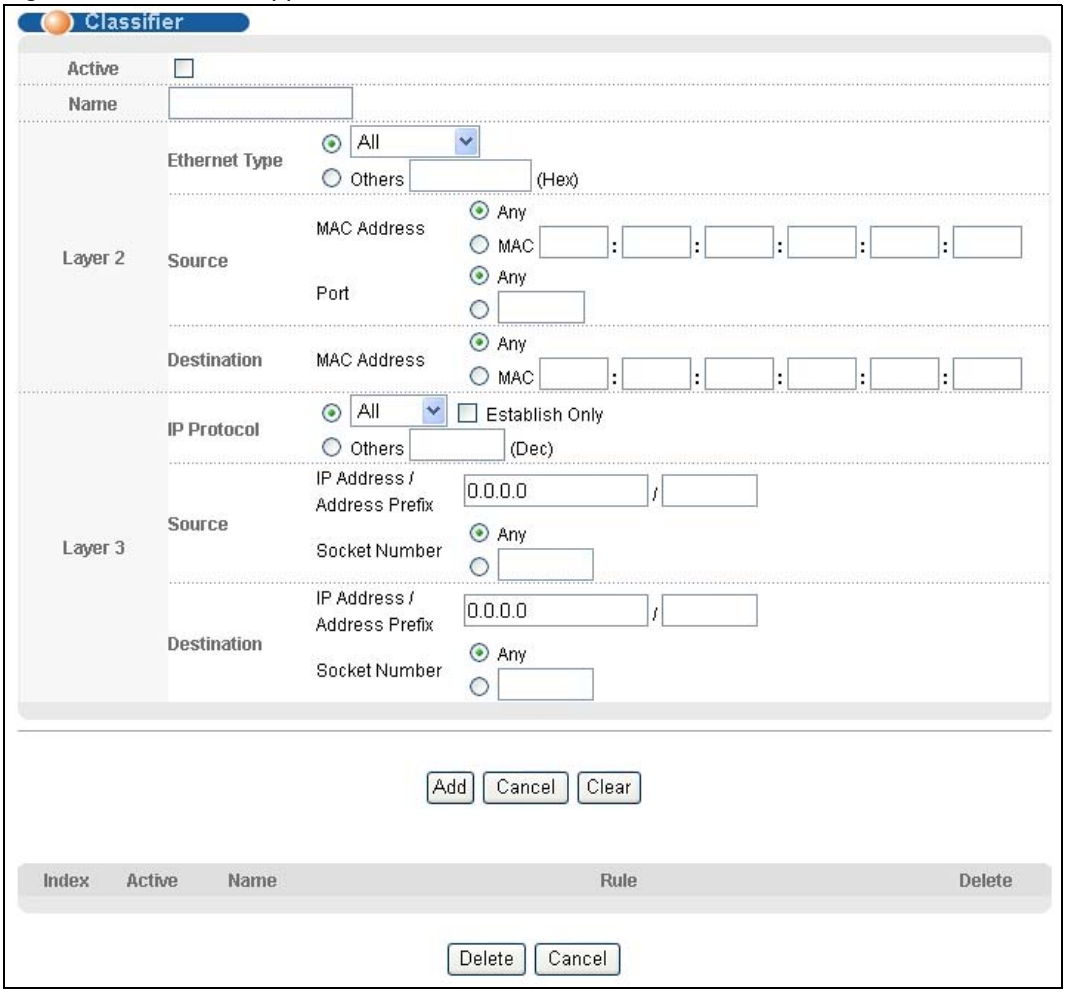
1. Configure classifiers to sort traffic into different flows.
2. Configure policy rules to define actions to be performed on a classified traffic flow (refer to Chapter 21 on page 160 to configure policy rules).

20.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to Chapter 21 on page 160.

Click **Advanced Application** > **Classifier** in the navigation panel to display the configuration screen as shown.

Figure 96 Advanced Application > Classifier



The following table describes the labels in this screen.

Table 48 Advanced Application > Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Layer 2 Specify the fields below to configure a layer 2 classifier.	
Ethernet Type	Select an Ethernet type or select **Other** and enter the Ethernet type number in hexadecimal value. Refer to Table 50 on page 157 for information.
Source	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (**Any**).

Table 48 Advanced Application > Classifier (continued)

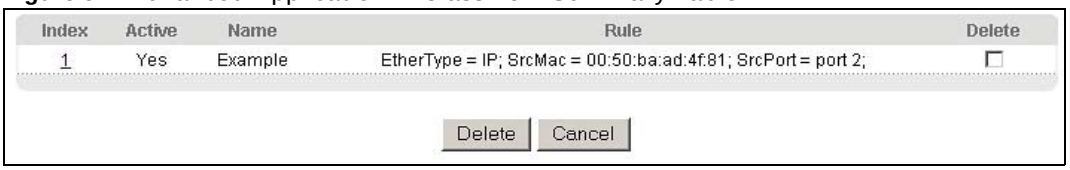
LABEL	DESCRIPTION
Destination	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
IP Protocol	Select an IP protocol type or select **Other** and enter the protocol number in decimal value. Refer to Table 51 on page 157 for more information. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask. A subnet mask can be represented in a 32-bit notation. For example, the subnet mask “255.255.255.0” can be represented as “11111111.11111111.11111111.00000000”, and counting up the number of ones in this case results in 24.
Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Refer to Table 52 on page 158 for more information.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Refer to Table 52 on page 158 for more information.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.

20.2.1 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.

Note: When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

Figure 97 Advanced Application > Classifier: Summary Table



The following table describes the labels in this screen.

Table 49 Classifier: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 50 Common Ethernet Types and Protocol Numbers

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

In the Internet Protocol there is a field, called "Protocol", to identify the next level protocol. The following table shows some common protocol types and the corresponding protocol number. Refer to http://www.iana.org/assignments/protocol-numbers for a complete list.

Table 51 Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17

Table 51 Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
EGP	8
L2TP	115

Some of the most common TCP and UDP port numbers are:

Table 52 Common TCP and UDP Port Numbers

PROTOCOL NAME	TCP/UDP PORT NUMBER
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110

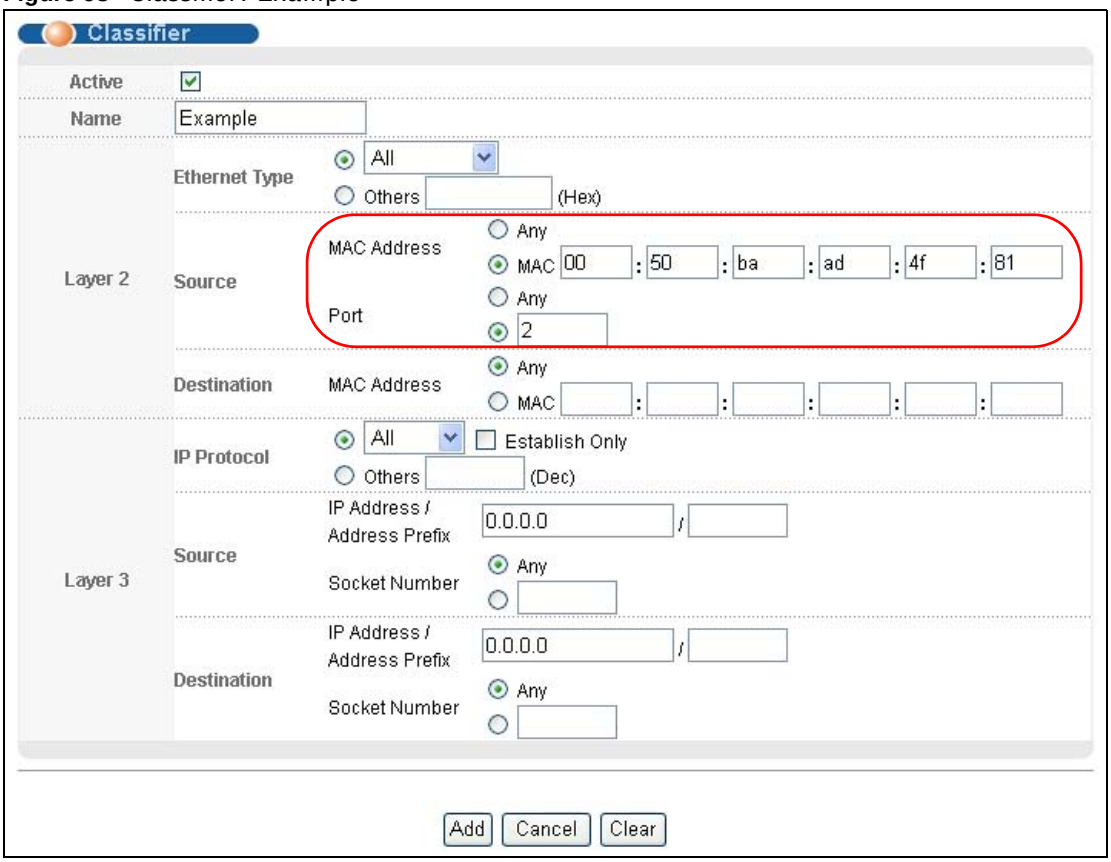
See Appendix B on page 317 for information on commonly used port numbers.

20.3 Classifier Example

The following screen shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define action(s) on the classified traffic flow.

Figure 98 Classifier: Example



21

Policy Rule

21.1 Policy Rules Overview

This chapter shows you how to configure policy rules.

A classifier distinguishes traffic into flows based on the configured criteria (refer to Chapter 20 on page 154 for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

21.1.1 What You Can Do

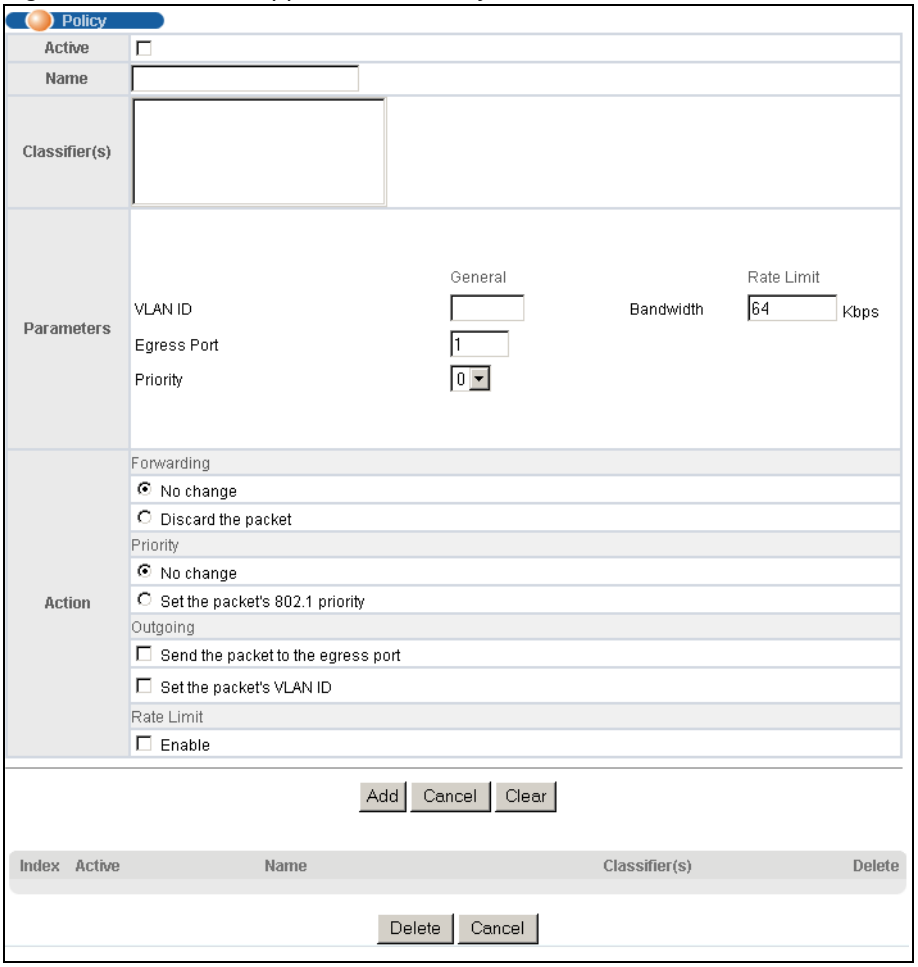
Use the **Policy** screen (Section 21.2 on page 160) to enable the policy and display the active classifier(s) you configure in the **Classifier** screen.

21.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to Section 20.2 on page 154 for more information.

Click **Advanced Applications** > **Policy Rule** in the navigation panel to display the screen as shown.

Figure 99 Advanced Application > Policy Rule



The following table describes the labels in this screen.

Table 53 Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the **Classifier** screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the **Action** field.	
General	
VLAN ID	Specify a VLAN ID number.
Egress Port	Type the number of an outgoing port.
Priority	Specify a priority level.

Table 53 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Rate Limit	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is dropped.
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 64 and 1000000.
Action Specify the action(s) the Switch takes on the associated classified traffic flow. Note: You can specify only one action (pair) in a policy rule. To have the Switch take multiple actions on the same traffic flow, you need to define multiple classifiers with the same criteria and apply different policy rules. Say you have several classifiers that identify the same traffic flow and you specify a different policy rule for each. If their policy actions conflict (**Discard the packet**, **Send the packet to the egress port** and **Rate Limit**), the Switch only applies the policy rules with the **Discard the packet** and **Send the packet to the egress port** actions depending on the classifier names. The longer the classifier name, the higher the classifier priority. If two classifier names are the same length, the bigger the character, the higher the classifier priority. The lowercase letters (such as a and b) have higher priority than the capitals (such as A and B) in the classifier name. For example, the classifier with the name of class 2, class a or class B takes priority over the classifier with the name of class 1 or class A. Let's say you set two classifiers (Class 1 and Class 2) and both identify all traffic from MAC address 11:22:33:44:55:66 on port 3. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to foward the packets to the egress port, the Switch will forward the packets. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will discard the packets immediately. If Policy 1 applies to Class 1 and the action is to foward the packets to the egress port, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will forward the packets.	
Forwarding	Select **No change** to forward the packets. Select **Discard the packet** to drop the packets.
Priority	Select **No change** to keep the priority setting of the frames. Select **Set the packet's 802.1 priority** to replace the packet's 802.1 priority field with the value you set in the Priority field.
Outgoing	Select **Send the packet to the egress port** to send the packet to the egress port. Select **Set the packet's VLAN ID** to replace the VLAN ID of the packets with the value you configure in the **VLAN ID** field.
Rate Limit	Select **Enable** to activate bandwidth limitation on the traffic flow(s).
Add	Click **Add** to inset the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays **Yes** when policy is activated and **No** when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click **Delete** to remove the selected entry from the summary table.

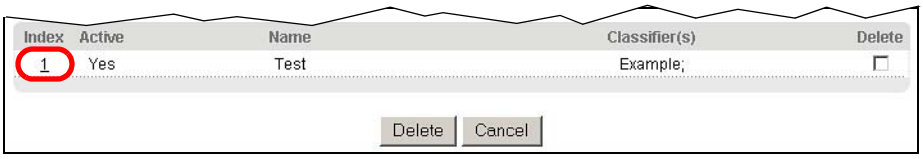
Table 53 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Delete	Click **Cancel** to clear the **Delete** check boxes.
Cancel	This field displays the policy index number. Click an index number to edit the policy.

21.2.1 Viewing and Editing Policy Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Policy** screen. To change the settings of a rule, click a number in the **Index** field.

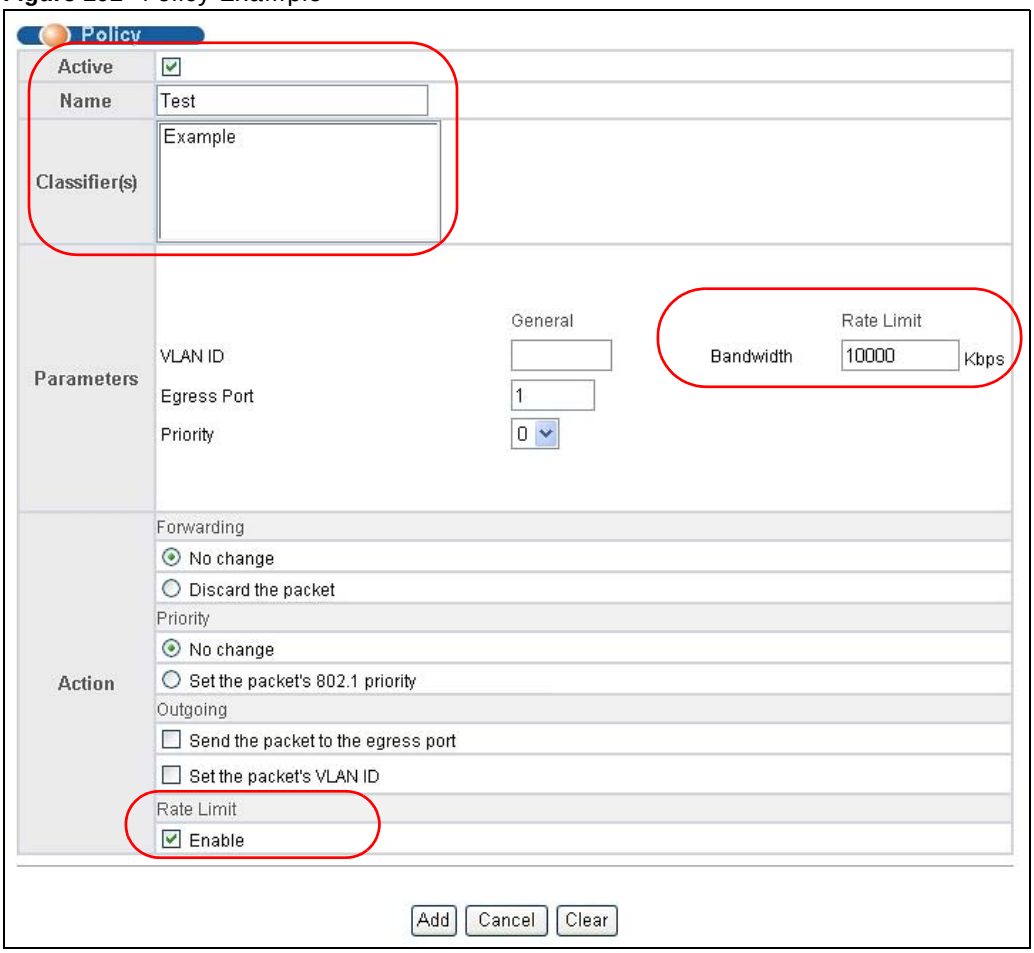
Figure 100 Advanced Application > Policy Rule: Summary Table



21.3 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth on a traffic flow classified using the **Example** classifier (refer to Section 20.3 on page 158).

Figure 101 Policy Example



22

Queuing Method

22.1 Overview

This chapter introduces the queuing methods supported.

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

22.1.1 What You Can Do

Use the **Queueing Method** screen (Section 22.2 on page 166) set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

22.1.2 What You Need to Know

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

Strictly Priority Queuing

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

Weighted Fair Queuing

Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (portion) (the number you configure in the Weight field) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on. Guaranteed quantum is calculated as Queue Weight x 2048 bytes.

Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given

an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

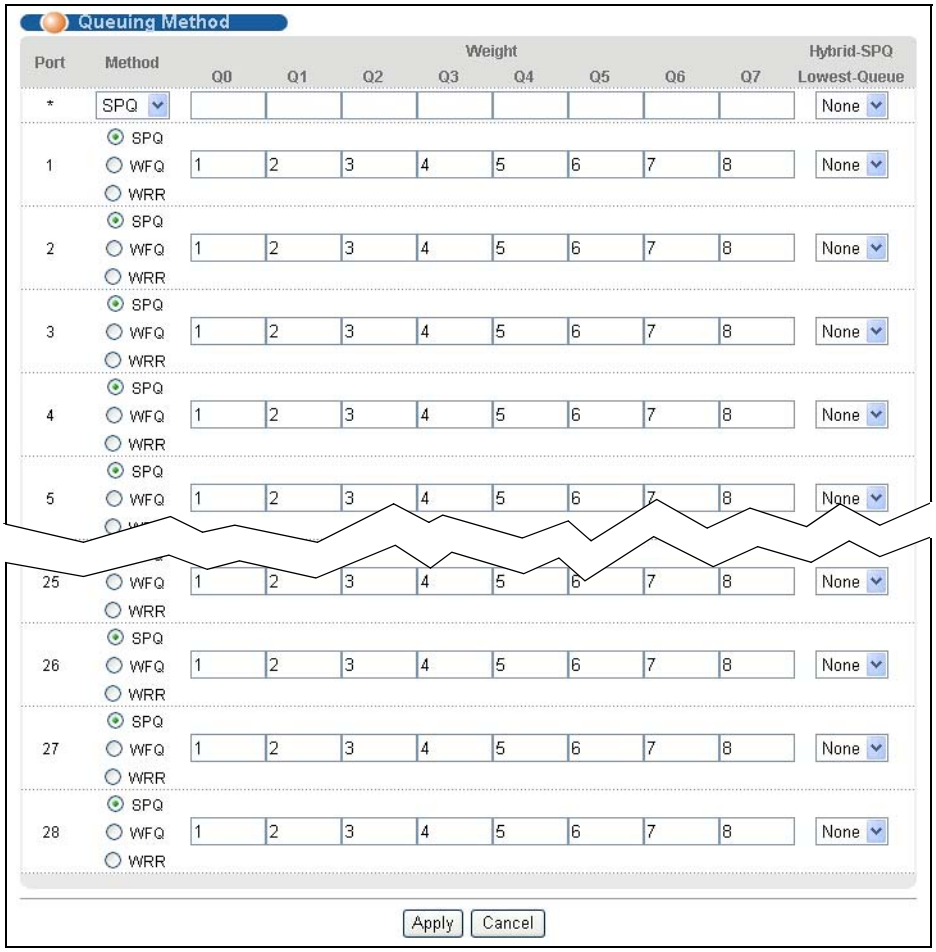
Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

22.2 Configuring Queuing

Use this screen to set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

Click **Advanced Application** > **Queuing Method** in the navigation panel.

Figure 102 Advanced Application > Queuing Method



The following table describes the labels in this screen.

Table 54 Advanced Application > Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Method	Select **SPQ** (Strictly Priority Queuing), **WFQ** (Weighted Fair Queuing) or **WRR** (Weighted Round Robin). Strictly Priority Queuing services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the **Weight** field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Weight	When you select **WFQ** or **WRR** enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
Hybrid-SPQ Lowest-Queue	This field is applicable only when you select **WFQ** or **WRR**. Select a queue (**Q0** to **Q7**) to have the Switch use **SPQ** to service the subsequent queue(s) after and including the specified queue for the port. For example, if you select **Q5**, the Switch services traffic on **Q5**, **Q6** and **Q7** using **SPQ**. Select **None** to always use **WFQ** or **WRR** for the port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23

Multicast

23.1 Overview

This chapter shows you how to configure various multicast features.

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

23.1.1 What You Can Do

- Use the **Multicast Status** screen (Section 23.2 on page 170) to view multicast group information.
- Use the **Multicast Setting** screen (Section 23.3 on page 171) to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
- Use the **IGMP Snooping VLAN** screen (Section 23.4 on page 174) to Configure how the Switch learns multicast group membership information and add VLANs upon which the Switch is to perform IGMP snooping.
- Use the **IGMP Filtering Profile** screen (Section 23.5 on page 175) to specify a range of multicast groups that clients connected to the Switch are able to join.
- Use the **MVR** screens (Section 23.6 on page 176) to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN.

23.1.2 What You Need to Know

Read on for concepts on Multicasting that can help you configure the screens in this chapter.

IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

IGMP Snooping

A Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing

through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

MVR Overview

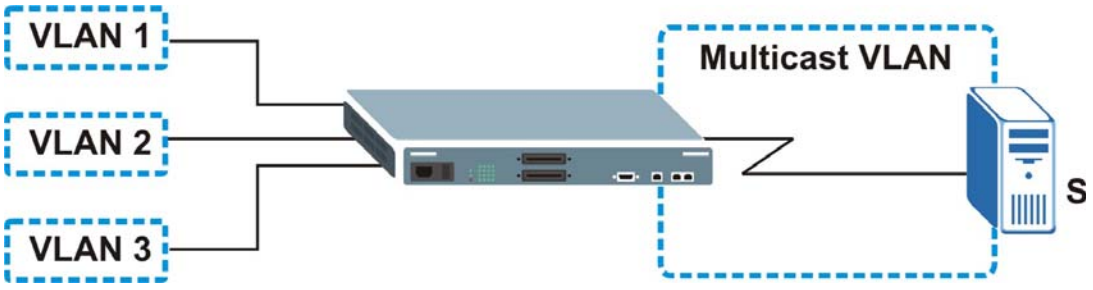
Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

Figure 103 MVR Network Example



Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, an uplink port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

Figure 104 MVR Multicast Television Example

23.2 Multicast Status

Click **Advanced Applications > Multicast** to display the screen as shown. This screen shows the multicast group information. See Section 23.1 on page 168 for more information on multicasting.

Figure 105 Advanced Application > Multicast

The following table describes the labels in this screen.

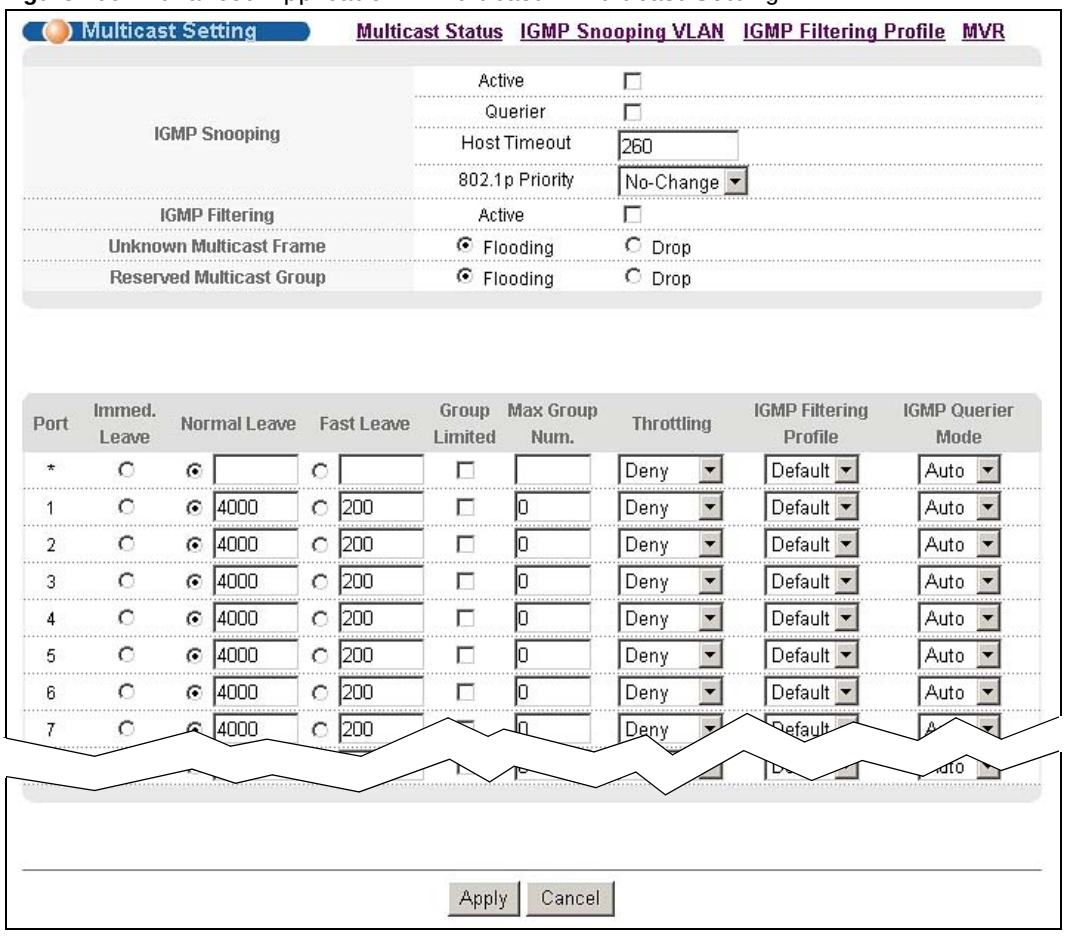
Table 55 Advanced Application > Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

23.3 Multicast Setting

Click **Advanced Applications > Multicast > Multicast Setting** link to display the screen as shown. See Section 23.1 on page 168 for more information on multicasting.

Figure 106 Advanced Application > Multicast > Multicast Setting



The following table describes the labels in this screen.

Table 56 Advanced Application > Multicast > Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP Snooping.
Active	Select **Active** to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Host Timeout	Specify the time (from 1 to 16,711,450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select **No-Change** to not replace the priority.
IGMP Filtering	Select **Active** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. Note: If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer 2 multicast MAC addresses used by Cisco layer 2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6,348,800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Fast Leave	Enter an IGMP fast leave timeout value (from 200 to 6,348,800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.

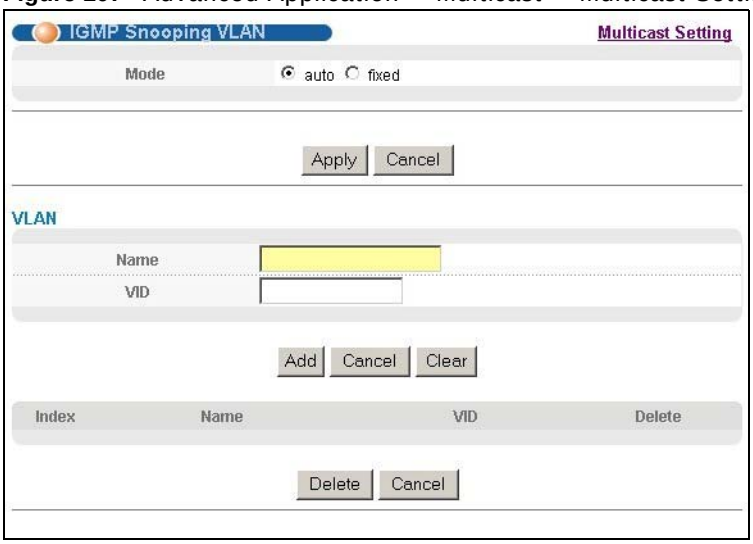
Table 56 Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
Max Group Num.	Enter the number (0-255) of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select **Deny** to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select **Replace** to replace an existing entry in the multicast forwarding table with the new IGMP report(s) received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select **Auto** to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select **Fixed** to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select **Edge** to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.4 IGMP Snooping VLAN

Click **Advanced Applications > Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See IGMP Snooping and VLANs on page 169 for more information on IGMP Snooping VLAN.

Figure 107 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN



The following table describes the labels in this screen.

Table 57 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	Select **auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **fixed** to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs (including up to three VLANs you configured in the **MVR** screen). For example, if you have configured one multicast VLAN in the **MVR** screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. Note: You must also enable IGMP snooping in the **Multicast Setting** screen first.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094. Note: You cannot configure the same VLAN ID as in the **MVR** screen.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.

Table 57 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN (continued)

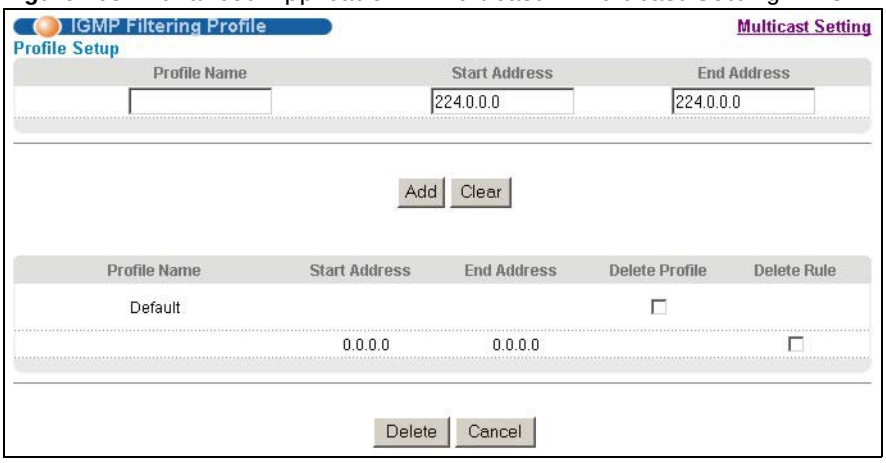
LABEL	DESCRIPTION
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click this to clear the fields.
Index	This is the number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

23.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **Multicast Setting** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **Advanced Applications** > **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** link to display the screen as shown.

Figure 108 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile



The following table describes the labels in this screen.

Table 58 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.

Table 58 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile (continued)

LABEL	DESCRIPTION
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
Add	Click **Add** to save the profile to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

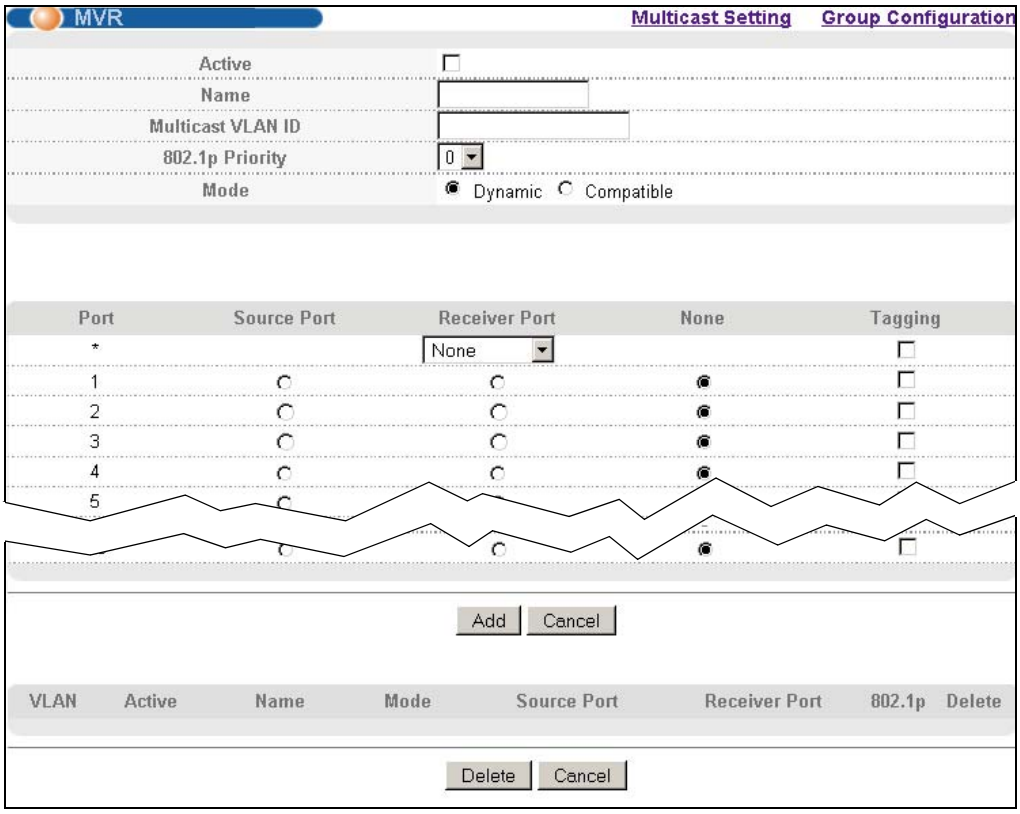
23.6 The MVR Screen

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Applications > Multicast** > **Multicast Setting > MVR** link to display the screen as shown next.

Note: You can create up to three multicast VLANs and up to 256 multicast rules on the Switch.

Note: Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 109 Advanced Application > Multicast > Multicast Setting > MVR



The following table describes the related labels in this screen.

Table 59 Advanced Application > Multicast > Multicast Setting > MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 English keyboard characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the Switch not to send IGMP reports.
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 59 Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

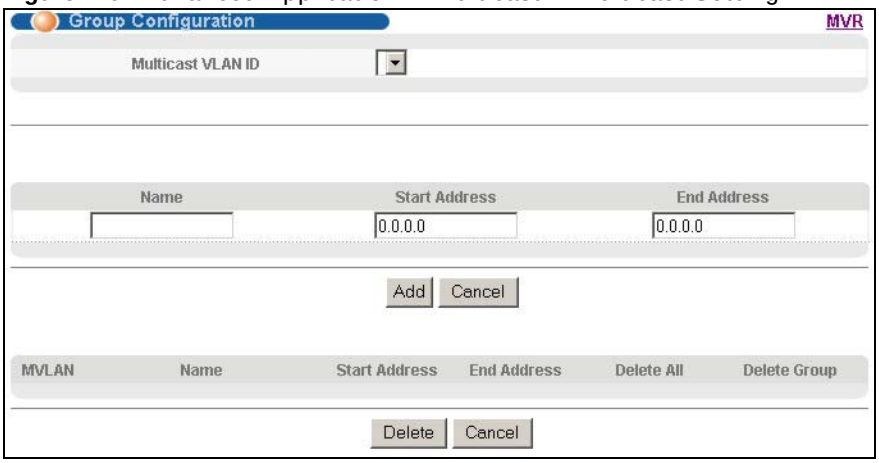
23.6.1 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.

Note: A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 110 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration



The following table describes the labels in this screen.

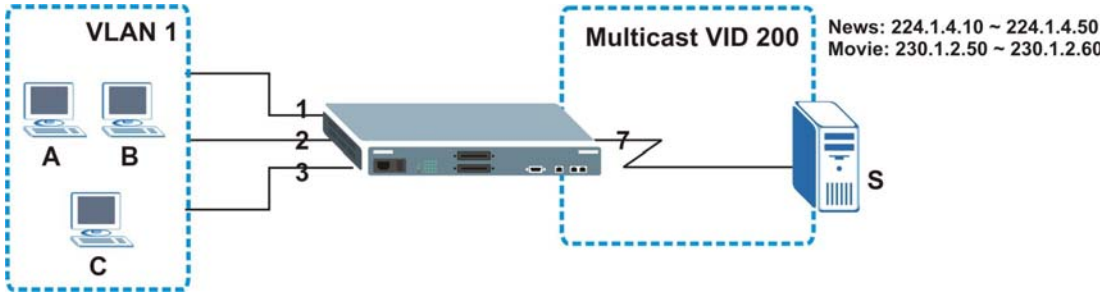
Table 60 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to IP Multicast Addresses on page 168 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group. Refer to IP Multicast Addresses on page 168 for more information on IP multicast addresses.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select **Delete Group** and click **Delete** to remove the selected entry(ies) from the table.
Cancel	Select **Cancel** to clear the checkbox(es) in the table.

23.6.2 MVR Configuration Example

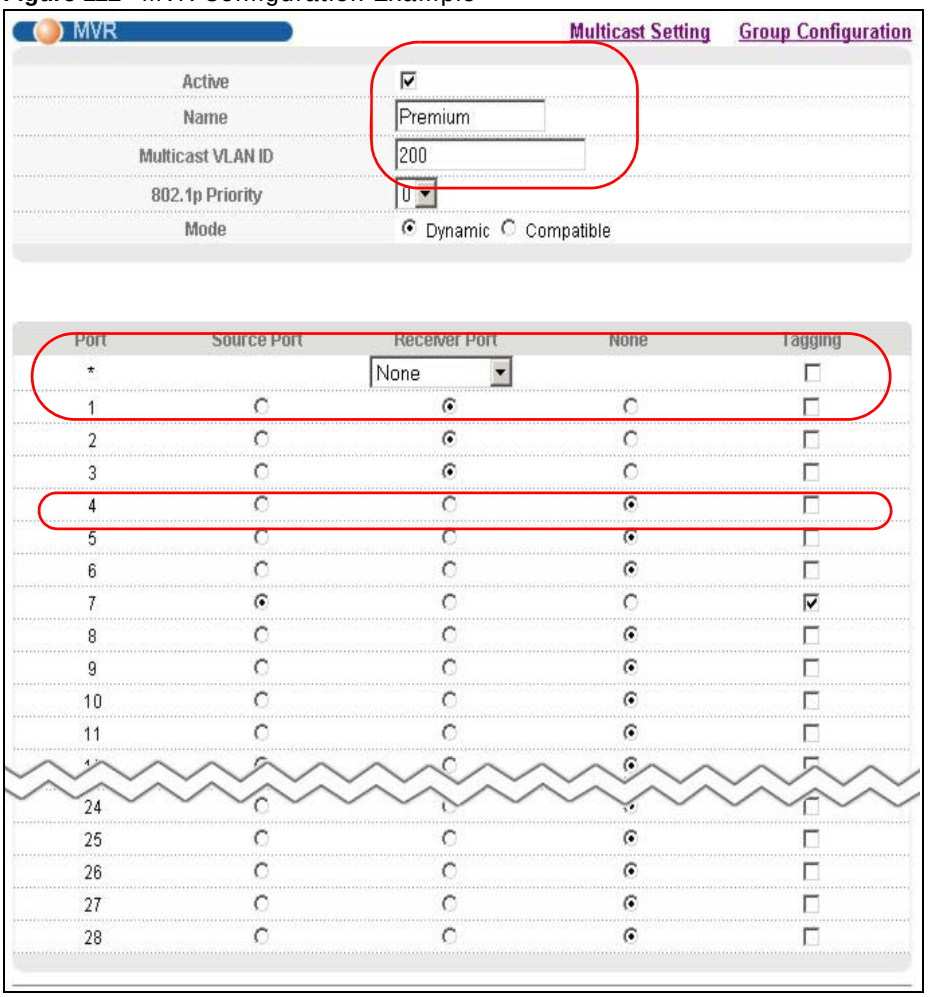
The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN 1 are able to receive the traffic.

Figure 111 MVR Configuration Example



To configure the MVR settings on the Switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 112 MVR Configuration Example



To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 113 MVR Group Configuration Example

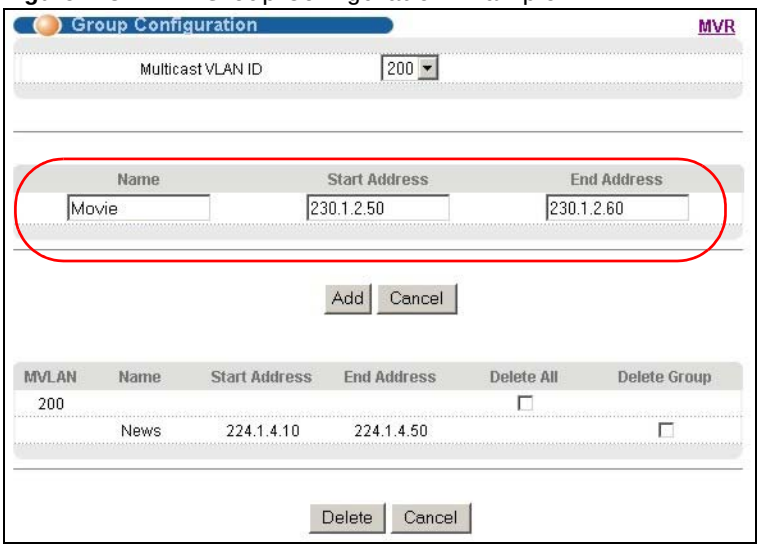
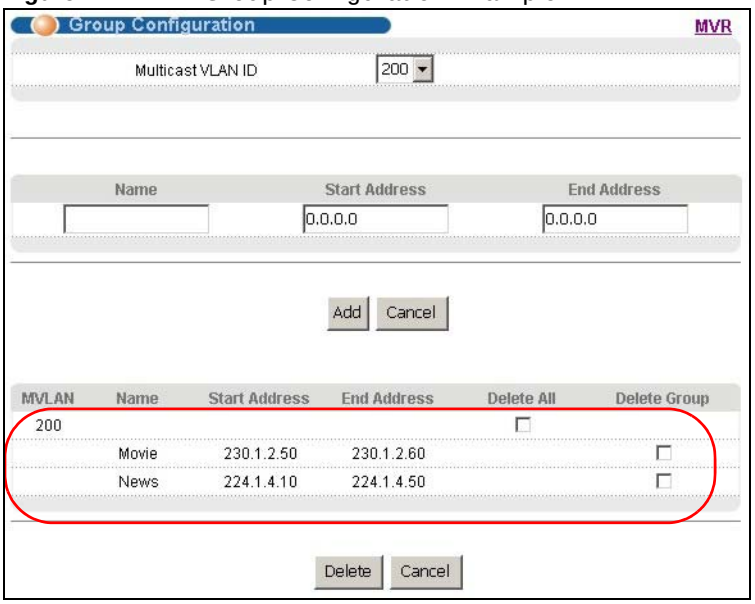


Figure 114 MVR Group Configuration Example



24

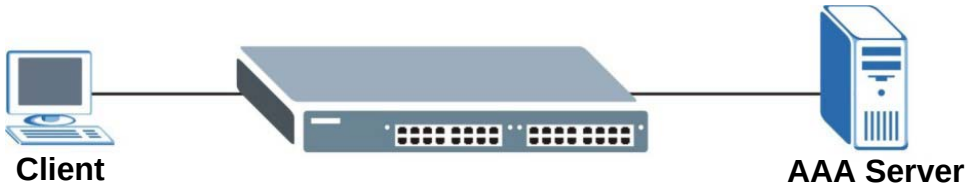
AAA

24.1 Overview

This chapter describes how to configure authentication and authorization settings on the Switch.

The external servers that perform authentication and authorization functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see Section on page 183) and TACACS+ (Terminal Access Controller Access-Control System Plus, see Section on page 183) as external authentication and authorization servers.

Figure 115 AAA Server



24.1.1 What You Can Do

- Use the **AAA** screen (Section 24.2 on page 183) to enable authentication and authorization or both of them on the Switch.
- use the **RADIUS Server Setup** screen (Section 24.3 on page 183) to configure your RADIUS server settings.
- Use the **TACACS+ Server Setup** screen (Section 24.4 on page 186) to configure your TACACS+ authentication settings.
- Use the **AAA Setup** screen (Section 24.5 on page 188) to specify the methods used to authenticate users accessing the Switch and specify which database the Switch should use first.

24.1.2 What You Need to Know

Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See Chapter 34 on page 255).

RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 61 RADIUS vs. TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

24.2 AAA Screens

The **AAA** screens allow you to enable authentication and authorization or both of them on the Switch. First, configure your authentication server settings (RADIUS, TACACS+ or both) and then set up the authentication priority, activate authorization.

Click **Advanced Application** > **AAA** in the navigation panel to display the screen as shown.

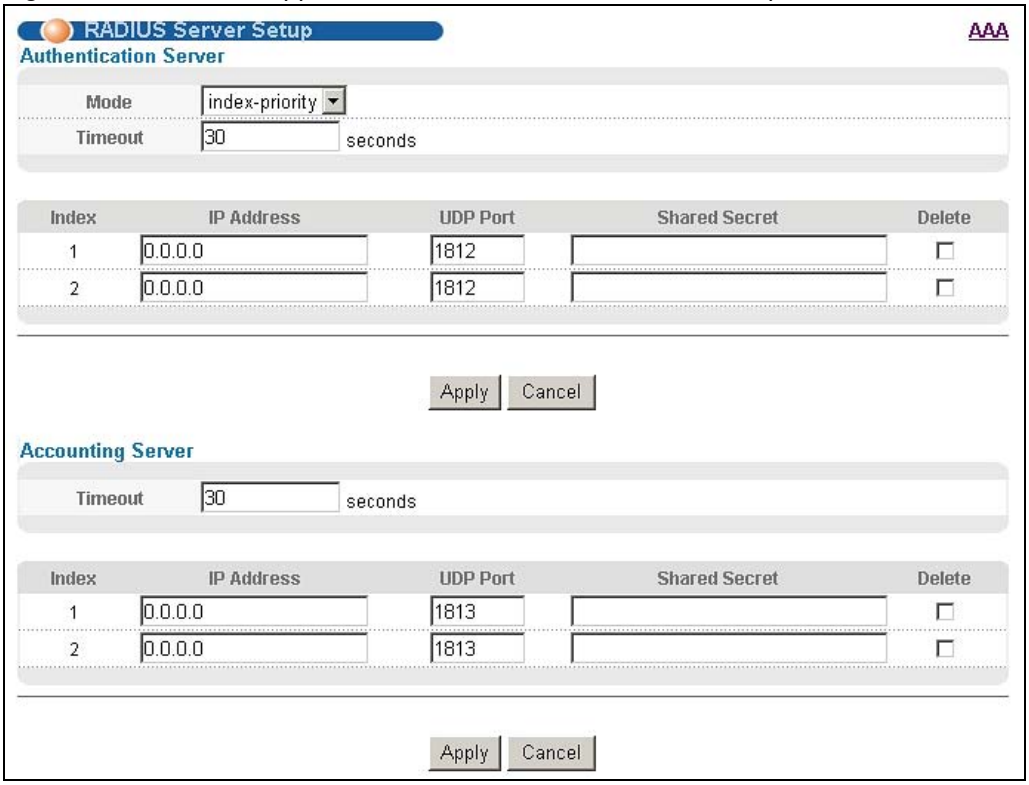
Figure 116 Advanced Application > AAA

24.3 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See Section on page 183 for more information on RADIUS servers and Section 24.6.2 on page 191 for RADIUS attributes utilized by

the authentication features on the Switch. Click on the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 117 Advanced Application > AAA > RADIUS Server Setup



The following table describes the labels in this screen.

Table 62 Advanced Application > AAA > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field is only valid if you configure multiple RADIUS servers. Select **index-priority** and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server. Select **round-robin** to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server. If you are using **index-priority** for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.

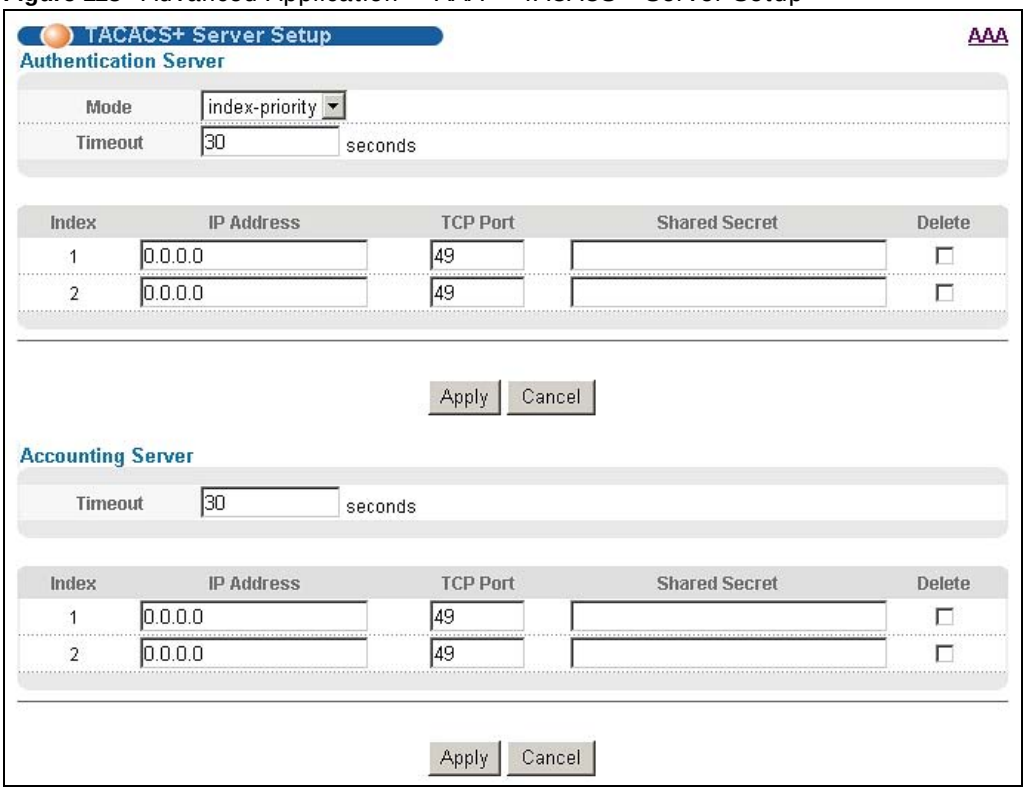
Table 62 Advanced Application > AAA > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS accounting server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.4 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See Section on page 183 for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 118 Advanced Application > AAA > TACACS+ Server Setup



The following table describes the labels in this screen.

Table 63 Advanced Application > AAA > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your TACACS+ authentication settings.
Mode	This field is only valid if you configure multiple TACACS+ servers. Select **index-priority** and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server. Select **round-robin** to alternate between the TACACS+ servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server. If you are using **index-priority** for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.

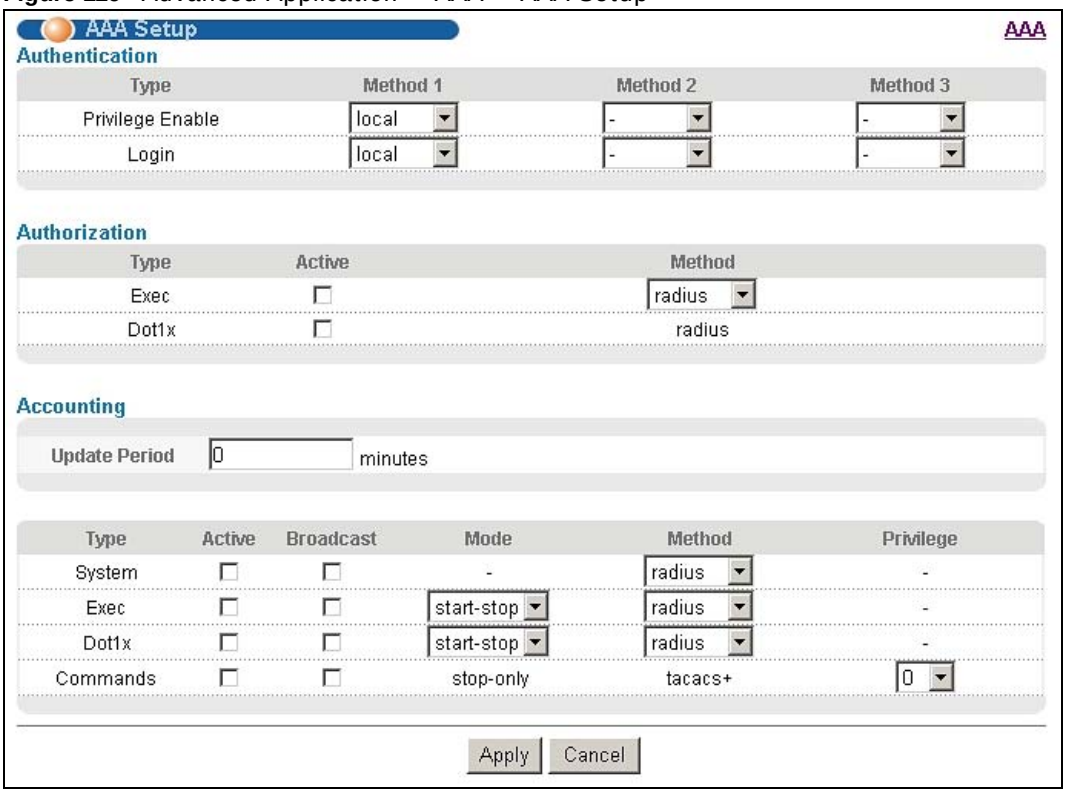
Table 63 Advanced Application > AAA > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
TCP Port	The default port of a TACACS+ server for authentication is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Accounting Server	Use this section to configure your TACACS+ accounting settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the TACACS+ server.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IP address of an external TACACS+ accounting server in dotted decimal notation.
TCP Port	The default port of a TACACS+ accounting server is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.5 AAA Setup

Use this screen to configure authentication and authorization settings on the Switch. Click on the **AAA Setup** link in the **AAA** screen to view the screen as shown.

Figure 119 Advanced Application > AAA > AAA Setup



The following table describes the labels in this screen.

Table 64 Advanced Application > AAA > AAA Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Privilege Enable	These fields specify which database the Switch should use (first, second and third) to authenticate access privilege level for administrator accounts (users for Switch management). Configure the access privilege of accounts via commands (See the CLI Reference Guide) for **local** authentication. The **TACACS+** and **RADIUS** are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate the access privilege level of administrators. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for access privilege level specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the access privilege configured for local authentication. Select **radius** or **tacacs+** to have the Switch check the access privilege via the external servers.

Table 64 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the **Access Control > Logins** screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for administrator accounts, specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the administrator accounts configured in the **Access Control > Logins** screen. Select **radius** to have the Switch check the administrator accounts configured via your RADIUS server. Select **tacacs+** to have the Switch check the administrator accounts configured via your TACACS+ server.
Authorization	Use this section to configure authorization settings on the Switch.
Type	Set whether the Switch provides the following services to a user. • **Exec**: Allow an administrator which logs in the Switch through Telnet, SSH or FTP to have different access privilege level assigned via the external server. • **Dot1x**: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.
Active	Select this to activate authorization for a specified event types.
Method	Select whether you want to use RADIUS or TACACS+ for authorization of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the **start-stop** option for the **Exec** or **Dot1x** entries.
Type	The Switch supports the following types of events to be sent to the accounting server(s): • **System** - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled • **Exec** - Configure the Switch to send information when an administrator logs in and logs out via the console port, telnet or SSH. • **Dot1x** - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session. • **Commands** - Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.

Table 64 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Mode	The Switch supports two modes of recording login events. Select: • **start-stop** - to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the **Update Period**), and when a user ends a session. • **stop-only** - to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events. TACACS+ is the only method for recording **Commands** type of event.
Privilege	This field is only configurable for **Commands** type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on the Switch.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.6 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

24.6.1 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels (See the CLI Reference Guide for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID**: An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). ZyXEL's vendor ID is 890.
- **Vendor-Type**: A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data**: A value you want to assign to the setting.

Note: Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the Switch.

Table 65 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **1** Vendor-data = ingress rate (Kbps in decimal format)
Egress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **2** Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = **890** Vendor-Type = **3** Vendor-Data = "**shell:priv-lvl=**N" or Vendor-ID = **9** (CISCO) Vendor-Type = **1** (CISCO-AVPAIR) Vendor-Data = "**shell:priv-lvl=**N" where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

24.6.1.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that the bolded values in the table are fixed values as defined in RFC 3580.

Table 66 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = **VLAN(13)** Tunnel-Medium-Type = **802(6)** Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the Switch.

24.6.2 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication elements in a user profile, which is stored on the RADIUS server. This appendix lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication.

This section lists the attributes used by authentication functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

24.6.3 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

24.6.3.1 Attributes Used for Authenticating Privilege Access

User-Name

- The format of the User-Name attribute is **$enab#$**, where # is the privilege level (1-14).

User-Password

NAS-Identifier

NAS-IP-Address

24.6.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

24.6.3.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

25

IP Source Guard

25.1 Overview

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

25.1.1 What You Can Do

- Use the **IP Source Guard** screen (Section 25.2 on page 194) to look at the current bindings for DHCP snooping and ARP inspection.
- Use the **IP Source Guard Static Binding** screen (Section 25.3 on page 195) to manage static bindings for DHCP snooping and ARP inspection.
- Use the **DHCP Snooping** screen (Section 25.4 on page 196) to look at various statistics about the DHCP snooping database.
- Use this **DHCP Snooping Configure** screen (Section 25.5 on page 199) to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database.
- Use the **DHCP Snooping Port Configure** screen (Section 25.5.1 on page 201) to specify whether ports are trusted or untrusted ports for DHCP snooping.
- Use the **DHCP Snooping VLAN Configure** screen (Section 25.5.2 on page 203) to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.
- Use the **ARP Inspection Status** screen (Section 25.6 on page 204) to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet.
- Use the **ARP Inspection VLAN Status** screen (Section 25.7 on page 205) to look at various statistics about ARP packets in each VLAN.
- Use the **ARP Inspection Log Status** screen (Section 25.8 on page 206) to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
- Use the **ARP Inspection Configure** screen (Section 25.9 on page 207) to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log.

- Use the **ARP Inspection Port Configure** screen (Section 25.9.1 on page 208) to specify whether ports are trusted or untrusted ports for ARP inspection.
- Use the **ARP Inspection VLAN Configure** screen (Section 25.9.2 on page 210) to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN.

25.1.2 What You Need to Know

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

25.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

Figure 120 IP Source Guard

The following table describes the labels in this screen.

Table 67 IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).

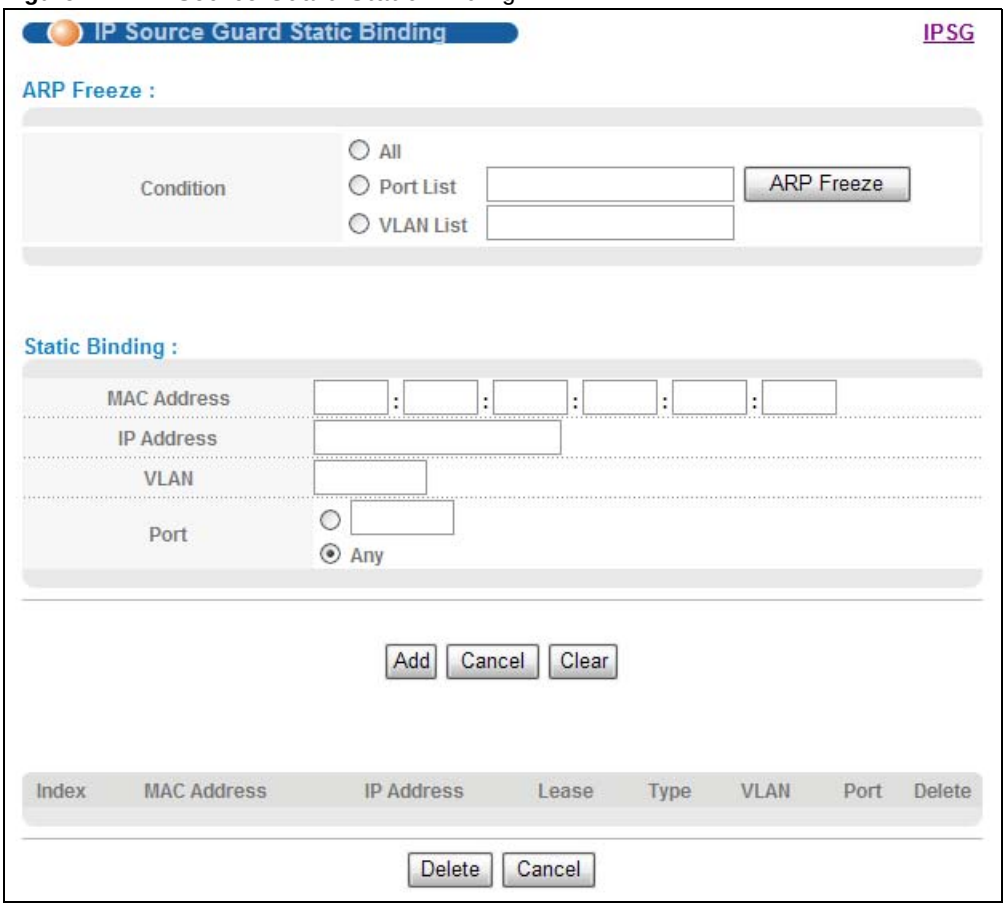
Table 67 IP Source Guard (continued)

LABEL	DESCRIPTION
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator. **dhcp-snooping**: This binding was learned by snooping DHCP packets.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

25.3 IP Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

Figure 121 IP Source Guard Static Binding



The following table describes the labels in this screen.

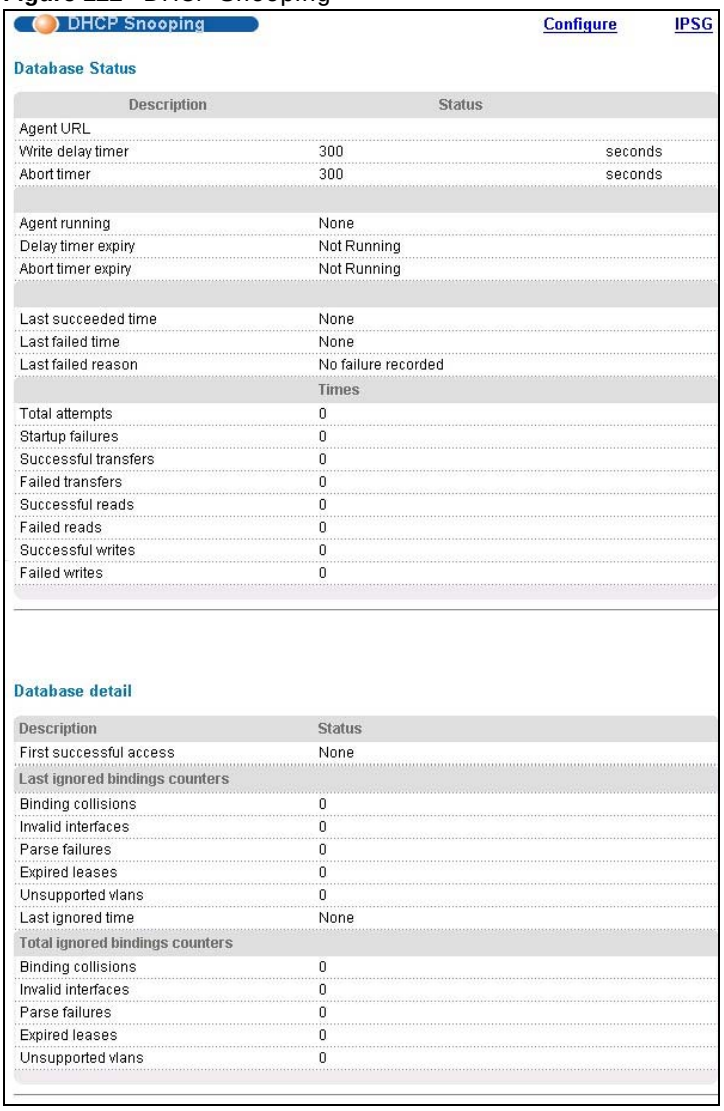
Table 68 IP Source Guard Static Binding

LABEL	DESCRIPTION
ARP Freeze	
Condition	Select one of the buttons and click **ARP Freeze** to create static bindings from previously learned ARP entries which match the criteria you specified. Select **All** to create static bindings from any previously learned ARP entries in the Switch's ARP table and add them in the IP source guard static binding table. Select **Port List** and enter the number of the port(s) to create static bindings from previously learned ARP entries which contain the specified port number and add them in the IP source guard static binding table. You can enter individual ports separated by a comma or a range of ports by using a dash. Select **VLAN List** and enter the VLAN ID(s) to create static bindings from previously learned ARP entries which contain the specified VLAN ID and add them in the IP source guard static binding table. You can enter individual VLAN IDs separated by a comma or a range of VLAN IDs by using a dash.
ARP Freeze	Click **ARP Freeze** to create static bindings from previously learned ARP entries which match the specified criteria and display them in the lower part of the screen.
Static Binding	
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select **Any**.
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Delete	Select this, and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

25.4 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping**.

Figure 122 DHCP Snooping



The following table describes the labels in this screen.

Table 69 DHCP Snooping

LABEL	DESCRIPTION
Database Status	This section displays the current settings for the DHCP snooping database. You can configure them in the **DHCP Snooping Configure** screen. See Section 25.5 on page 199.
Agent URL	This field displays the location of the DHCP snooping database.
Write delay timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.

Table 69 DHCP Snooping (continued)

LABEL	DESCRIPTION
Agent running	This field displays the status of the current update or access of the DHCP snooping database. **none**: The Switch is not accessing the DHCP snooping database. **read**: The Switch is loading dynamic bindings from the DHCP snooping database. **write**: The Switch is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays **Not Running** if the Switch is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays **Not Running** if the current bindings have not changed since the last update.
	This section displays information about the last time the Switch updated the DHCP snooping database.
Last succeeded time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.
Successful transfers	This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed transfers	This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful reads	This field displays the number of times the Switch read bindings from the DHCP snooping database successfully.
Failed reads	This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database.
Successful writes	This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully.
Failed writes	This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database.
Database detail	
First successful access	This field displays the first time the Switch accessed the DHCP snooping database for any reason.
Last ignored bindings counters	This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the CLI Reference Guide.
Binding collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.

Table 69 DHCP Snooping (continued)

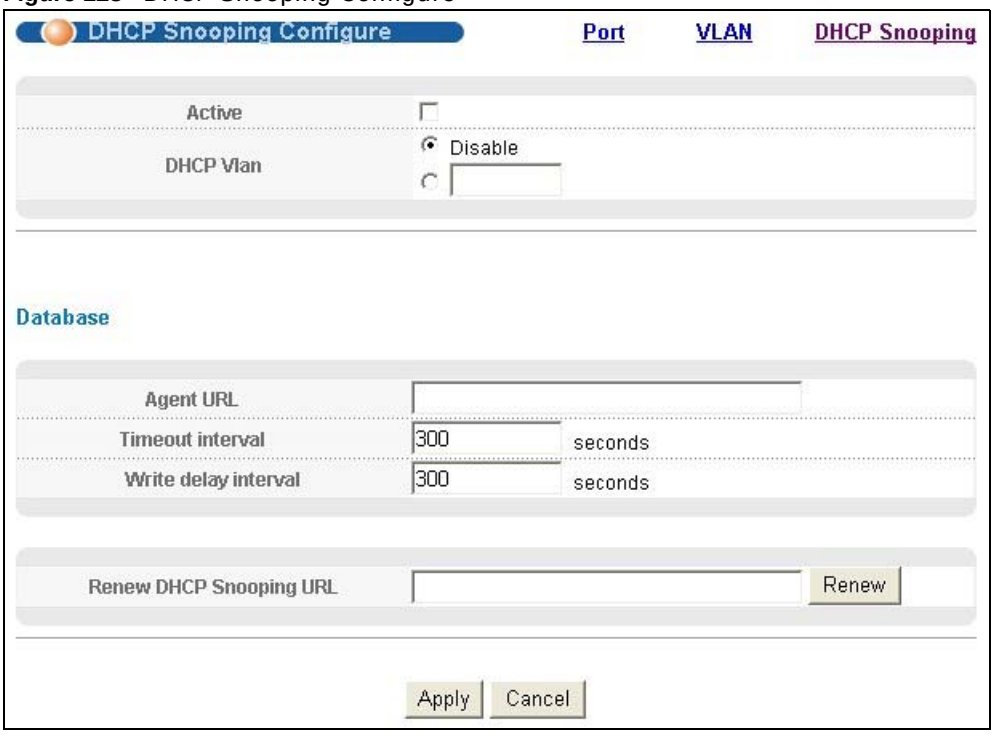
LABEL	DESCRIPTION
Parse failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total ignored bindings counters	This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the CLI Reference Guide.
Binding collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

25.5 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are

still available after a restart. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Figure 123 DHCP Snooping Configure



The following table describes the labels in this screen.

Table 70 DHCP Snooping Configure

LABEL	DESCRIPTION
Active	Select this to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
DHCP Vlan	Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can enable **Option82** in the **DHCP Snooping VLAN Configure** screen (Section 25.5.2 on page 203) to help the DHCP servers distinguish between DHCP requests from different VLAN. Select **Disable** if you do not want the Switch to forward DHCP packets to a specific VLAN.
Database	If **Timeout interval** is greater than **Write delay interval**, it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: **tftp://{domain name or IP address}/directory, if applicable/file name**; for example, **tftp://192.168.10.1/database.txt**.

Table 70 DHCP Snooping Configure (continued)

LABEL	DESCRIPTION
Timeout interval	Enter how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Write delay interval	Enter how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click **Renew** if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in **Agent URL**. When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the **Binding collisions** counter in the **DHCP Snooping** screen (Section 25.4 on page 196).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

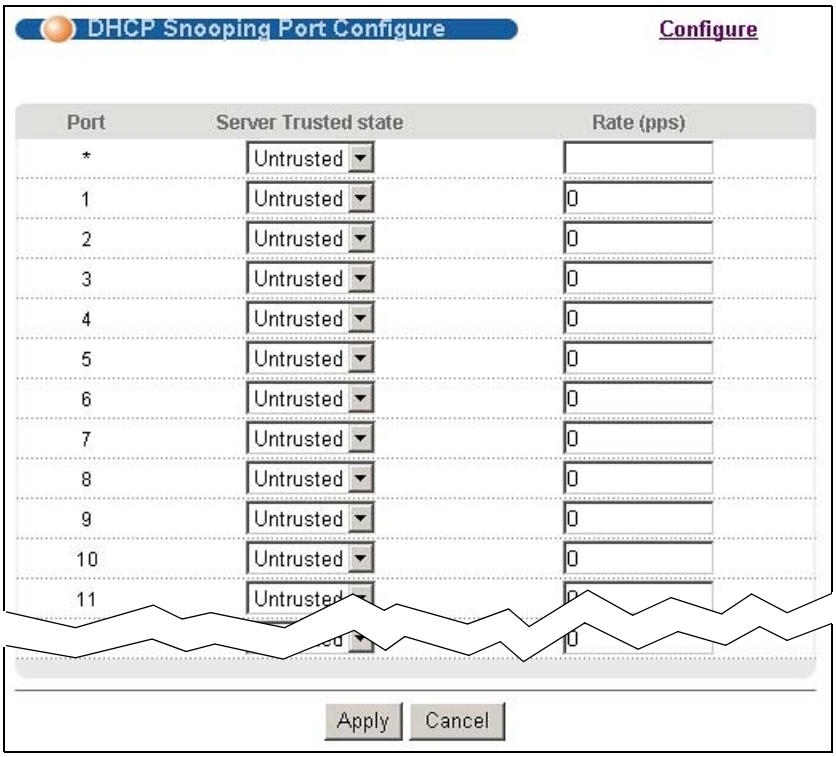
25.5.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

Note: If DHCP snooping is enabled but there are no trusted ports, DHCP requests cannot reach the DHCP server.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Figure 124 DHCP Snooping Port Configure



The following table describes the labels in this screen.

Table 71 DHCP Snooping Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the ***** port, the settings are applied to all of the ports.
Server Trusted state	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations: • The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the packet do not match any of the current bindings. • The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1-2048) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.

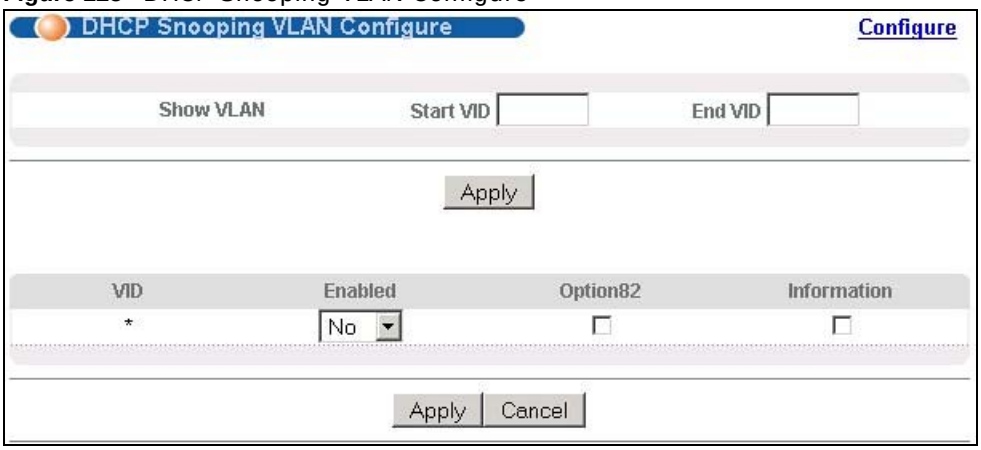
Table 71 DHCP Snooping Port Configure (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.5.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information (Chapter 32 on page 244) to DHCP requests that the Switch relays to a DHCP server for each VLAN. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

Figure 125 DHCP Snooping VLAN Configure



The following table describes the labels in this screen.

Table 72 DHCP Snooping VLAN Configure

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
Option82	Select this to have the Switch add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen. See Section 25.5 on page 199.
Information	Select this to have the Switch add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can configure the system name in the **General Setup** screen. See Chapter 8 on page 66. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen. See Section 25.5 on page 199.

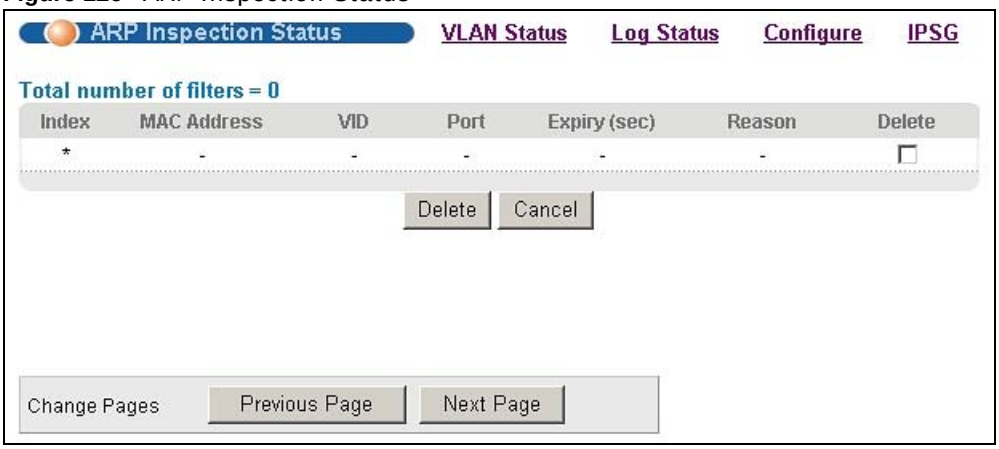
Table 72 DHCP Snooping VLAN Configure (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.6 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

Figure 126 ARP Inspection Status



The following table describes the labels in this screen.

Table 73 ARP Inspection Status

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (**Delete**).

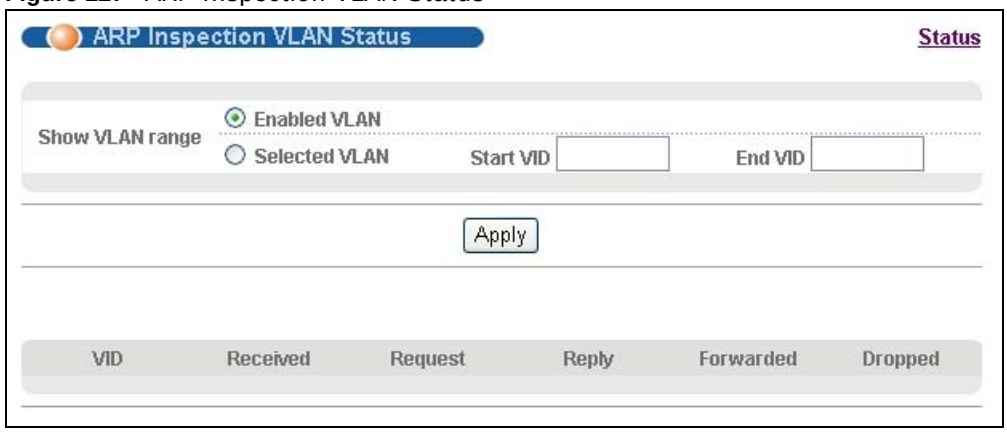
Table 73 ARP Inspection Status (continued)

LABEL	DESCRIPTION
Reason	This field displays the reason the ARP packet was discarded. **MAC+VLAN**: The MAC address and VLAN ID were not in the binding table. **IP**: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. **Port**: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select this, and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

25.7 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Figure 127 ARP Inspection VLAN Status



The following table describes the labels in this screen.

Table 74 ARP Inspection VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID (**Start VID**) and the highest VLAN ID (**End VID**) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.

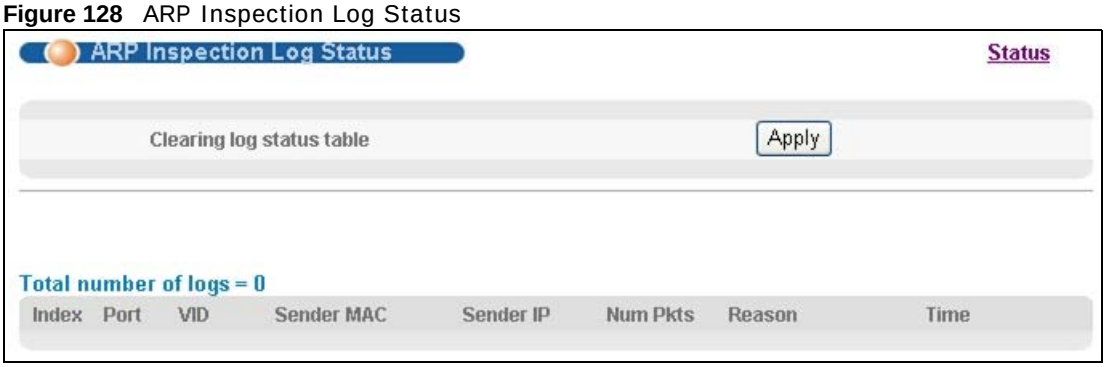
Table 74 ARP Inspection VLAN Status

LABEL	DESCRIPTION
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

25.8 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Figure 128 ARP Inspection Log Status



The following table describes the labels in this screen.

Table 75 ARP Inspection Log Status

LABEL	DESCRIPTION
Clearing log status table	Click **Apply** to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called **overflow** with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the **ARP Inspection Configure** screen. See Section 25.9 on page 207.

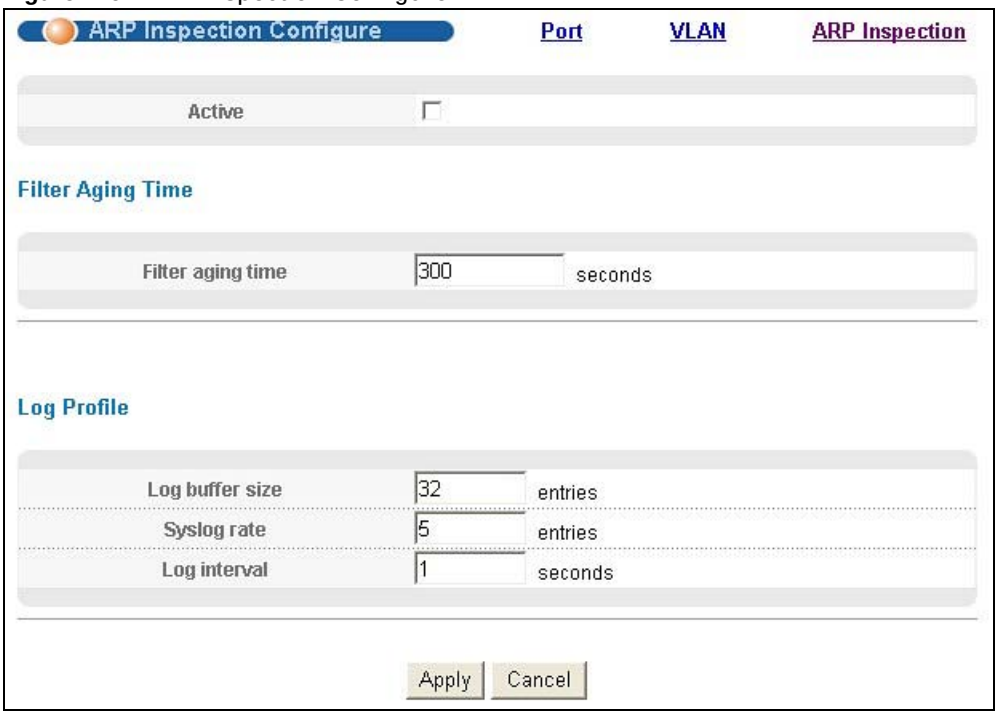
Table 75 ARP Inspection Log Status (continued)

LABEL	DESCRIPTION
Reason	This field displays the reason the log message was generated. **dhcp deny**: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. **static deny**: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. **deny**: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. **dhcp permit**: An ARP packet was forwarded because it matched a dynamic binding. **static permit**: An ARP packet was forwarded because it matched a static binding. In the **ARP Inspection VLAN Configure** screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 25.9.2 on page 210.
Time	This field displays when the log message was generated.

25.9 ARP Inspection Configure

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Figure 129 ARP Inspection Configure



The following table describes the labels in this screen.

Table 76 ARP Inspection Configure

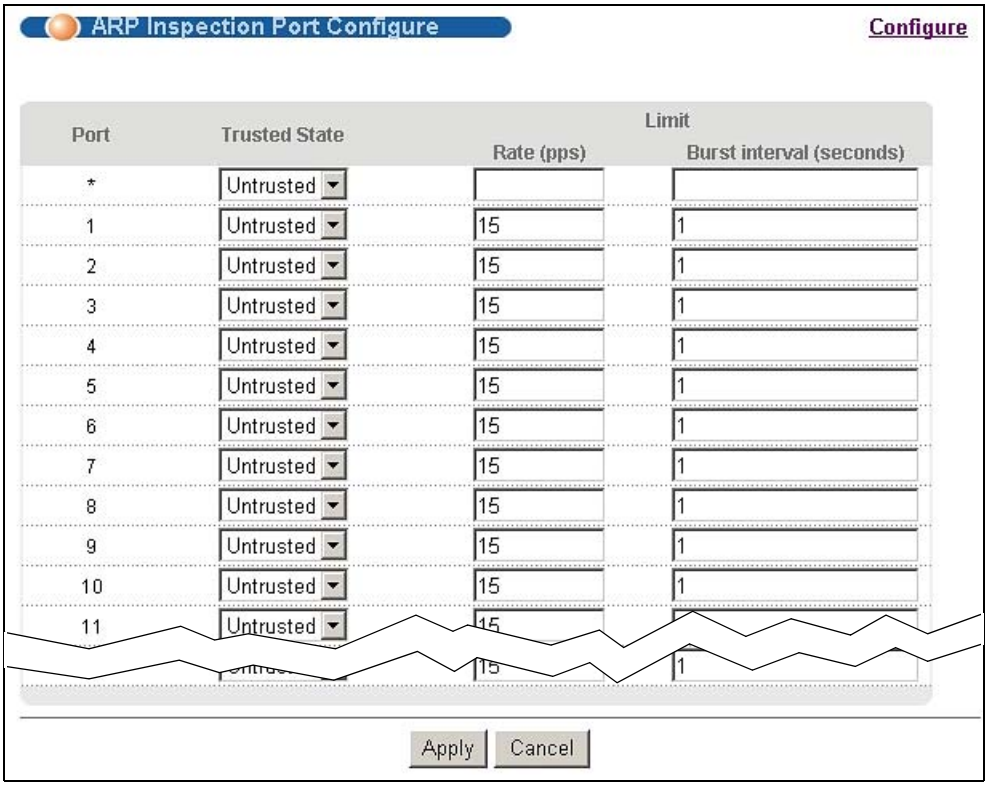
LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1~2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Enter 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1~1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified **Syslog rate** and **Log interval**. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click **Clearing log status table** in the **ARP Inspection Log Status** screen to clear the log and reset this counter. See Section 25.8 on page 206.
Syslog rate	Enter the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the **Log Interval**. You must configure the syslog server (Chapter 37 on page 287) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between **Syslog rate** and **Log interval** is illustrated in the following examples: • 4 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 1: the Switch sends 4 syslog messages every second. • 6 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 2: the Switch sends 5 syslog messages every 2 seconds.
Log interval	Enter how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See **Syslog rate** for an example of the relationship between **Syslog rate** and **Log interval**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.9.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the Switch receives ARP packets on each untrusted port. To

open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Figure 130 ARP Inspection Port Configure



The following table describes the labels in this screen.

Table 77 ARP Inspection Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the ***** port, the settings are applied to all of the ports.
Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	These settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1-2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1-15 seconds) of the burst interval.

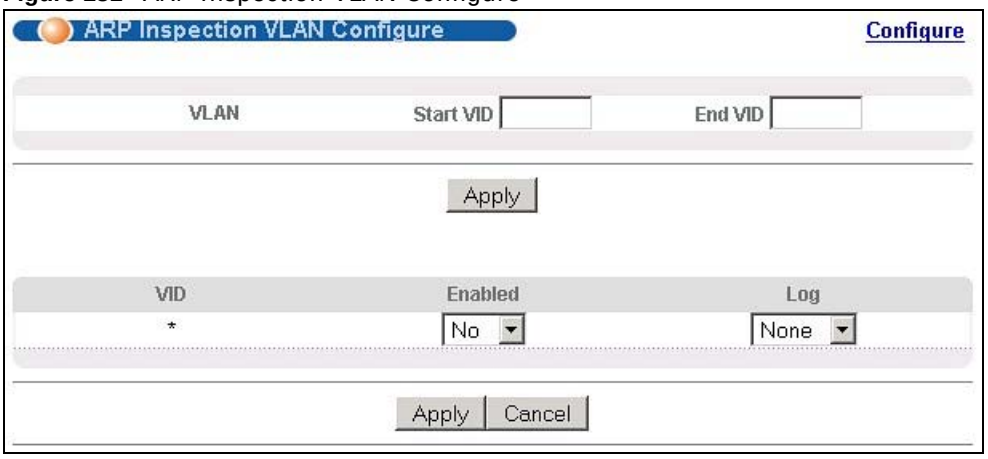
Table 77 ARP Inspection Port Configure (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.9.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Figure 131 ARP Inspection VLAN Configure



The following table describes the labels in this screen.

Table 78 ARP Inspection VLAN Configure

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable ARP inspection on the VLAN. Select **No** to disable ARP inspection on the VLAN.

Table 78 ARP Inspection VLAN Configure (continued)

LABEL	DESCRIPTION
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. **None**: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. **Deny**: The Switch generates log messages when it discards an ARP packet from the VLAN. **Permit**: The Switch generates log messages when it forwards an ARP packet from the VLAN. **All**: The Switch generates log messages every time it receives an ARP packet from the VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.10 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

25.10.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

25.10.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

25.10.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 132 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-..-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

25.10.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames. See Chapter 32 on page 244 for more information about DHCP relay option 82.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings (Chapter 32 on page 244).

25.10.1.4 Configuring DHCP Snooping

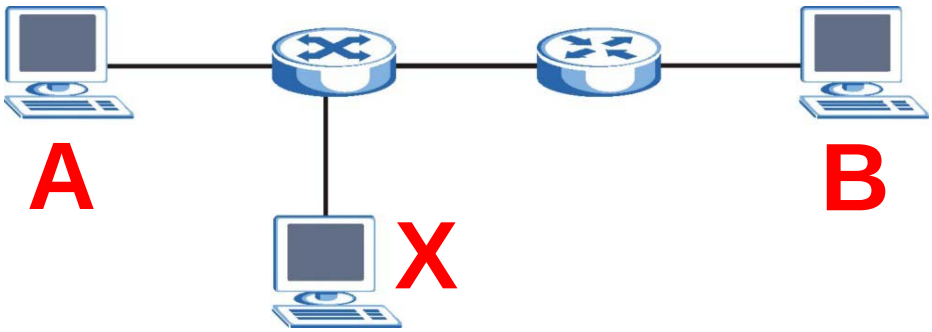
Follow these steps to configure DHCP snooping on the Switch.

1. Enable DHCP snooping on the Switch.
2. Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.
3. Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
4. Configure static bindings.

25.10.2 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 133 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

25.10.2.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters (Chapter 12 on page 107).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

25.10.2.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

25.10.2.3 Syslog

The Switch can send syslog messages to the specified syslog server (Chapter 37 on page 287) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

25.10.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1. Configure DHCP snooping. See Section 25.10.1.4 on page 213.

   Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

2. Enable ARP inspection on each VLAN.

3. Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

26

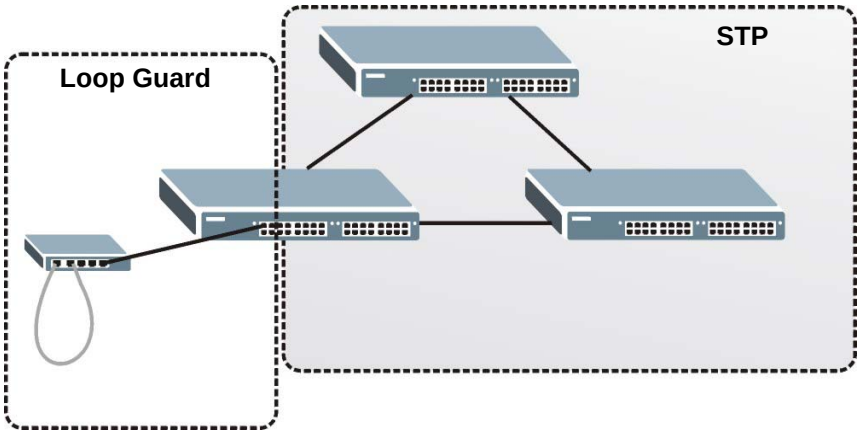
Loop Guard

26.1 Overview

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network. STP cannot prevent loops that occur on the edge of your network.

Figure 134 Loop Guard vs. STP



Refer to Section 26.1.2 on page 215 for more information.

26.1.1 What You Can Do

Use the **Loop Guard** screen (Section 26.2 on page 217) to enable loop guard on the Switch and in specific ports.

26.1.2 What You Need to Know

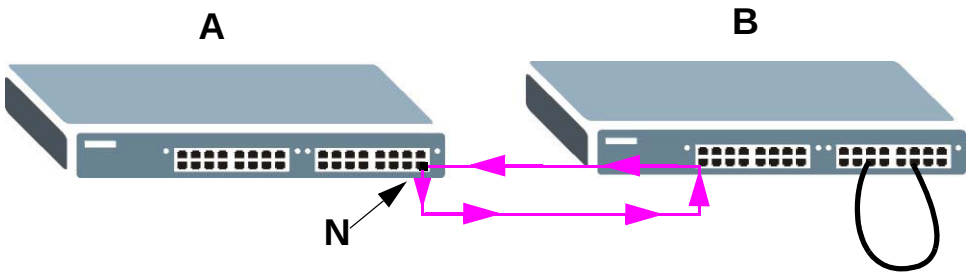
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from B.

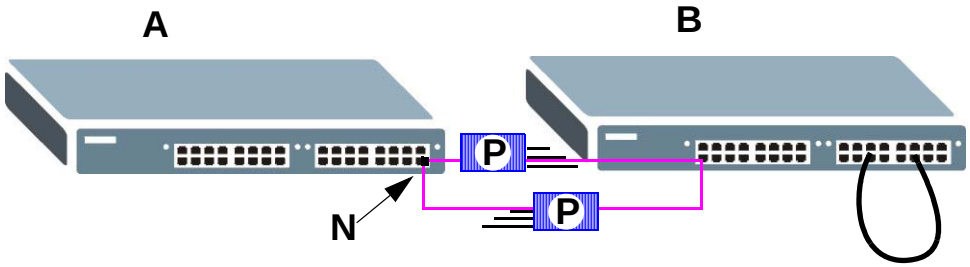
Figure 135 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

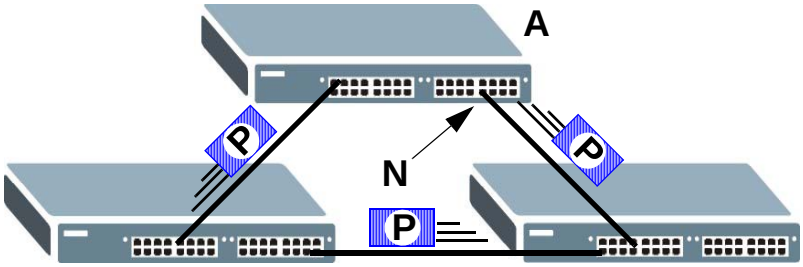
Figure 136 Loop Guard - Probe Packet



The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long

as loop guard is enabled on port **N**. The Switch will shut down port **N** if it detects that the probe packet has returned to the Switch.

Figure 137 Loop Guard - Network Loop



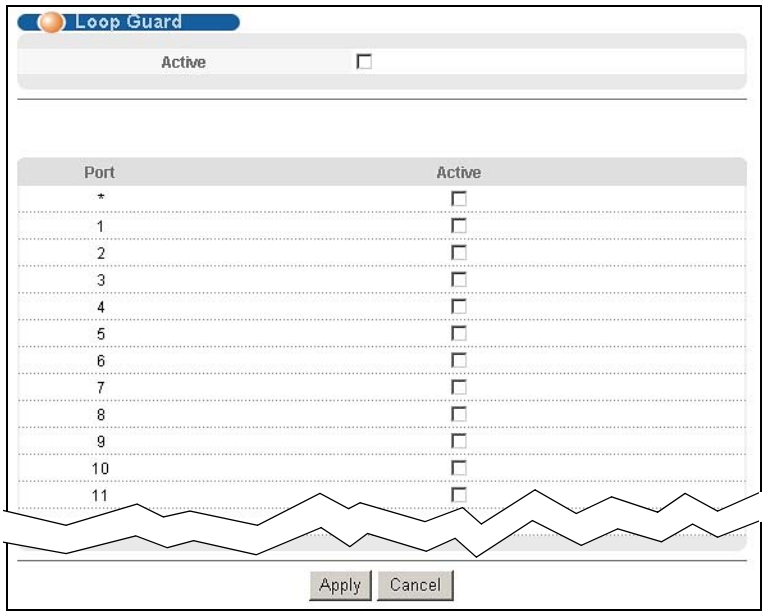
Note: After resolving the loop problem on your network you can re-activate the disabled port via the web configurator (see Section 8.7 on page 75) or via commands (See the CLI Reference Guide).

26.2 Loop Guard Setup

Click **Advanced Application** > **Loop Guard** in the navigation panel to display the screen as shown.

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 138 Advanced Application > Loop Guard



The following table describes the labels in this screen.

Table 79 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

27

Layer 2 Protocol Tunneling

27.1 Overview

This chapter shows you how to configure layer 2 protocol tunneling on the Switch.

27.1.1 What You Can Do

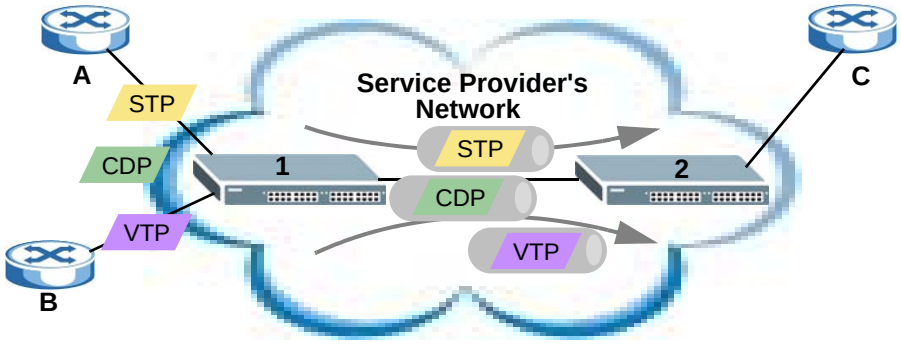
Use the **Layer 2 Protocol Tunnel** screen (Section 27.2 on page 221) to enable layer 2 protocol tunneling on the Switch and specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets.

27.1.2 What You Need to Know

Layer 2 protocol tunneling (L2PT) is used on the service provider's edge devices.

L2PT allows edge switches (**1** and **2** in the following figure) to tunnel layer 2 STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol) and VTP (VLAN Trunking Protocol) packets between customer switches (**A**, **B** and **C** in the following figure) connected through the service provider's network. The edge switch encapsulates layer 2 protocol packets with a specific MAC address before sending them across the service provider's network to other edge switches.

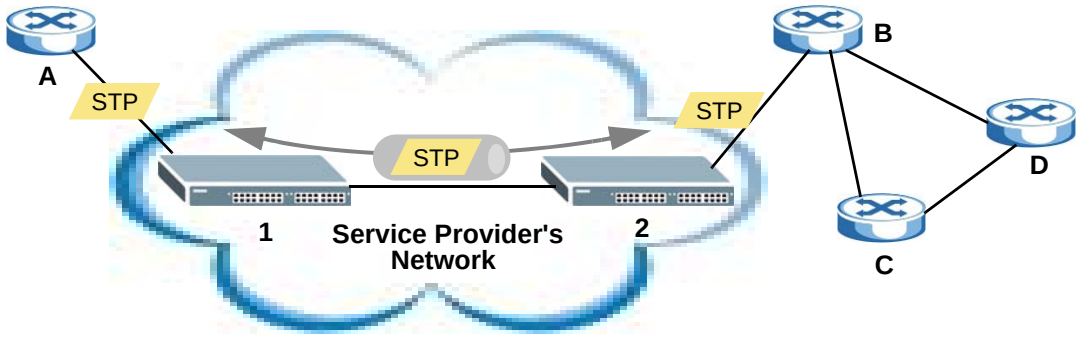
Figure 139 Layer 2 Protocol Tunneling Network Scenario



In the following example, if you enable L2PT for STP, you can have switches **A**, **B**, **C** and **D** in the same spanning tree, even though switch **A** is not directly connected to switches **B**, **C** and **D**. Topology change information can be propagated throughout the service provider's network.

To emulate a point-to-point topology between two customer switches at different sites, such as **A** and **B**, you can enable protocol tunneling on edge switches **1** and **2** for PAgP (Port Aggregation Protocol), LACP or UDLD (UniDirectional Link Detection).

Figure 140 L2PT Network Example



27.1.2.1 Layer 2 Protocol Tunneling Mode

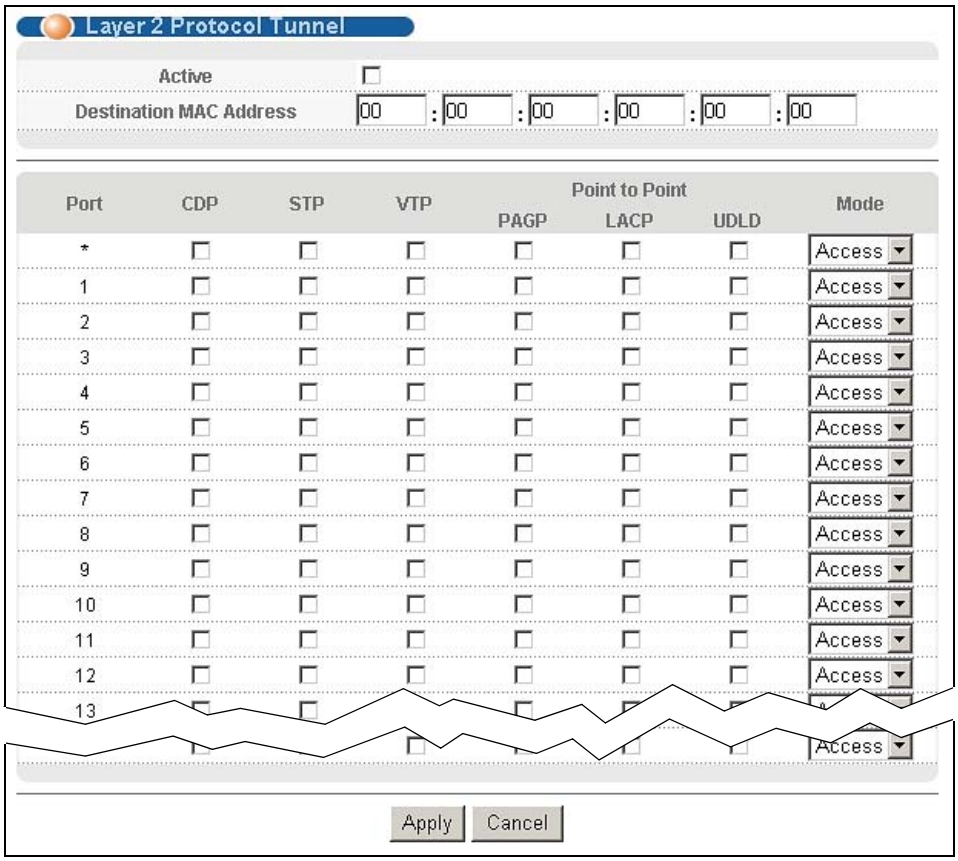
Each port can have two layer 2 protocol tunneling modes, **Access** and **Tunnel**.

- The **Access** port is an ingress port on the service provider's edge device (**1** or **2** in Figure 140 on page 220) and connected to a customer switch (**A** or **B**). Incoming layer 2 protocol packets received on an access port are encapsulated and forwarded to the tunnel ports.
- The **Tunnel** port is an egress port at the edge of the service provider's network and connected to another service provider's switch. Incoming encapsulated layer 2 protocol packets received on a tunnel port are decapsulated and sent to an access port.

27.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application** > **Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 141 Advanced Application > Layer 2 Protocol Tunneling



The following table describes the labels in this screen.

Table 80 Advanced Application > Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Select this to enable layer 2 protocol tunneling on the Switch.
Destination MAC Address	Specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets. Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network. Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 80 Advanced Application > Layer 2 Protocol Tunneling (continued)

LABEL	DESCRIPTION
CDP	Select this option to have the Switch tunnel CDP (Cisco Discovery Protocol) packets so that other Cisco devices can be discovered through the service provider's network.
STP	Select this option to have the Switch tunnel STP (Spanning Tree Protocol) packets so that STP can run properly across the service provider's network and spanning trees can be set up based on bridge information from all (local and remote) networks.
VTP	Select this option to have the Switch tunnel VTP (VLAN Trunking Protocol) packets so that all customer switches can use consistent VLAN configuration through the service provider's network.
Point to Point	The Switch supports PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. Both PAgP and UDLD are Cisco's proprietary data link layer protocols. PAgP is similar to LACP and used to set up a logical aggregation of Ethernet ports automatically. UDLD is to determine the link's physical status and detect a unidirectional link.
PAGP	Select this option to have the Switch send PAgP packets to a peer to automatically negotiate and build a logical port aggregation.
LACP	Select this option to have the Switch send LACP packets to a peer to dynamically creates and manages trunk groups.
UDLD	Select this option to have the Switch send UDLD packets to a peer's port it connected to monitor the physical status of a link.
Mode	Select **Access** to have the Switch encapsulate the incoming layer 2 protocol packets and forward them to the tunnel port(s). Select **Access** for ingress ports at the edge of the service provider's network. Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) only. Select **Tunnel** for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer 2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the service(s) is not enabled on an access port, the protocol packets are dropped.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

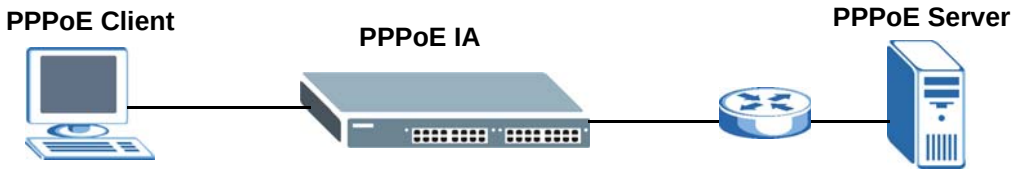
28

PPPoE

28.1 PPPoE Intermediate Agent Overview

This chapter describes how the Switch gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.



28.1.1 What You Can Do

- Use the **PPPoE** screen (Section 28.2 on page 225) to display the main PPPoE screen.
- Use the **Intermediate Agent** screen (Section 28.3 on page 226) to enable the PPPoE Intermediate Agent on the Switch.
- Use the PPPoE Per-**Port** screen (Section 28.3.1 on page 227) to set the port state and configure PPPoE intermediate agent sub-options on a per-port basis.
- Use the PPPoE Per-Port Per-**VLAN** screen (Section 28.3.2 on page 228) to configure PPPoE IA settings that apply to a specific VLAN on a port.
- Use the PPPoE for **VLAN** screen (Section 28.3.3 on page 230) to enable the PPPoE Intermediate Agent on a VLAN.

28.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

28.1.2.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 81 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the “ADSL Forum” IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client.

28.1.2.2 Sub-Option Format

There are two types of sub-option: “Agent Circuit ID Sub-option” and “Agent Remote ID Sub-option”. They have the following formats.

Table 82 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 83 PPPoE IA Remote ID Sub-option Format

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	MAC Address or String (63 bytes)

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. The Switch takes the Circuit ID string you manually configure for a VLAN on a port as the highest priority and the Circuit ID string for a port as the second priority. In addition, the Switch puts the PPPoE client’s MAC address into the Agent Remote ID Sub-option if you do not specify any user-defined string.

Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The variables can be the slot ID of the PPPoE client, the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

The identifier-string, slot ID, port number and VLAN ID are separated from each other by a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space. An Agent Circuit ID Sub-option example is “Switch/07/0123” and indicates the PPPoE packets come from a PPPoE client which is connected to the Switch’s port 7 and belong to VLAN 123.

Table 84 PPPoE IA Circuit ID Sub-option Format: Using Identifier String and Variables

SubOpt	Length	Value						
0x01 (1 byte)	N (1 byte)	Identifier String (53 byte)	delimiter (1 byte)	Slot ID (1 byte)	delimiter (1 byte)	Port No (2 byte)	delimiter (1 byte)	VLAN ID (4 bytes)

WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and disable the flexible Circuit ID syntax in the **PPPoE > Intermediate Agent** screen, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is

defined in the DSL Forum Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates “Ethernet”.

Table 85 PPPoE IA Circuit ID Sub-option Format: Defined in WT-101

SubOpt	Length	Value								
0x01 (1 byte)	N (1 byte)	Access Node Identifier (20 byte)	Space (1 byte)	eth (3 byte)	Space (1 byte)	Slot ID (1 byte)	/ (1 byte)	Port No (2 byte)	: (1 byte)	VLAN ID (4 bytes)

28.1.2.3 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s).

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

28.2 The PPPoE Screen

Use this screen to configure the PPPoE Intermediate Agent on the Switch.

Click **Advanced Application** > **PPPoE** in the navigation panel to display the screen as shown. Click **Click Here** to go to the **Intermediate Agent** screen.

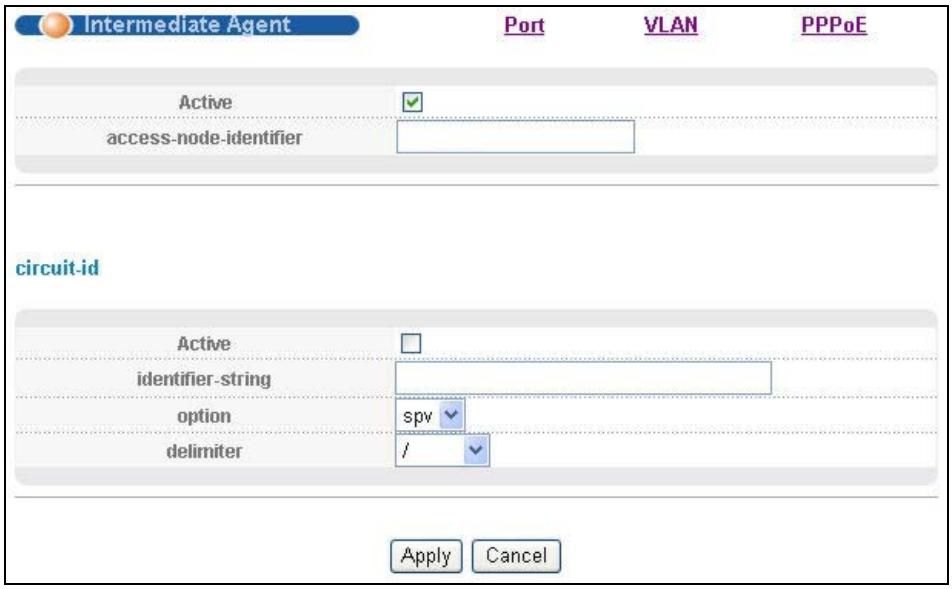
Figure 142 Advanced Application > PPPoE Intermediate Agent

28.3 PPPoE Intermediate Agent

Use this screen to configure the Switch to give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.

Click **Advanced Application** > **PPPoE > Intermediate Agent** in the navigation panel to display the screen as shown.

Figure 143 Advanced Application > PPPoE > Intermediate Agent



The following table describes the labels in this screen.

Table 86 Advanced Application > PPPoE > Intermediate Agent

LABEL	DESCRIPTION
Active	Select this option to enable the PPPoE intermediate agent globally on the Switch.
access-node-identifier	Enter up to 20 ASCII characters to identify the PPPoE intermediate agent. Hyphens (-) and spaces are also allowed. The default is the Switch's host name.
circuit-id	Use this section to configure the Circuit ID field in the PADI and PADR packets. The Circuit ID you configure for a specific port or for a specific VLAN on a port has priority over this. The Circuit ID you configure for a specific port (in the **Advanced Application > PPPoE > Intermediate Agent > Port** screen) or for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has priority over this. That means, if you also want to configure PPPoE IA Per-Port or Per-Port Per-VLAN setting, leave the fields here empty and configure circuit-id and remote-id in the Per-Port or Per-Port Per-VLAN screen.
Active	Select this option to have the Switch add the user-defined identifier string and variables (specified in the **option** field) to PADI or PADR packets from PPPoE clients. If you leave this option unselected and do not configure any Circuit ID string (using CLI commands) on the Switch, the Switch will use the string specified in the **access-node-identifier** field.
identifier-string	Specify a string that the Switch adds in the Agent Circuit ID sub-option. You can enter up to 53 ASCII characters. Spaces are allowed.

Table 86 Advanced Application > PPPoE > Intermediate Agent (continued)

LABEL	DESCRIPTION
option	Select the variables that you want the Switch to generate and add in the Agent Circuit ID sub-option. The variable options include **sp**, **sv**, **pv** and **spv** which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively. The Switch enters a zero into the PADI and PADR packets for the slot value.
delimiter	Select a delimiter to separate the identifier-string, slot ID, port number and/or VLAN ID from each other. You can use a pound key (**#**), semi-colon (**;**), period (**.**), comma (**,**), forward slash (**/**) or space.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

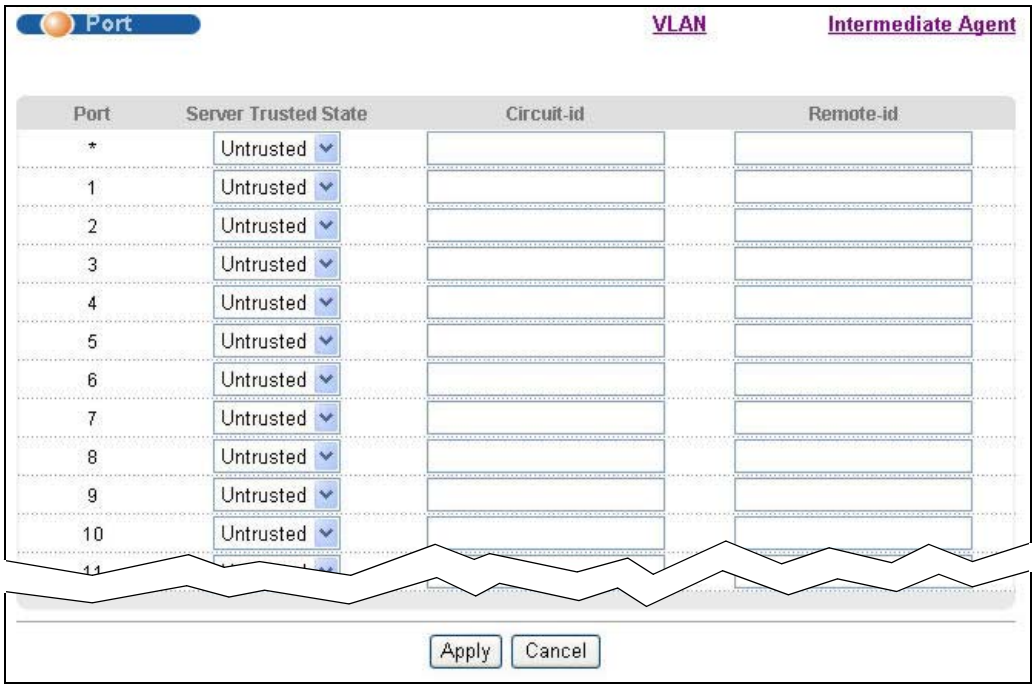
28.3.1 PPPoE IA Per-Port

Use this screen to specify whether individual ports are trusted or untrusted ports and have the Switch add extra information to PPPoE discovery packets from PPPoE clients on a per-port basis.

Note: The Switch will drop all PPPoE packets if you enable the PPPoE Intermediate Agent on the Switch and there are no trusted ports.

Click the **Port** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 144 Advanced Application > PPPoE > Intermediate Agent > Port



The following table describes the labels in this screen.

Table 87 Advanced Application > PPPoE > Intermediate Agent > Port

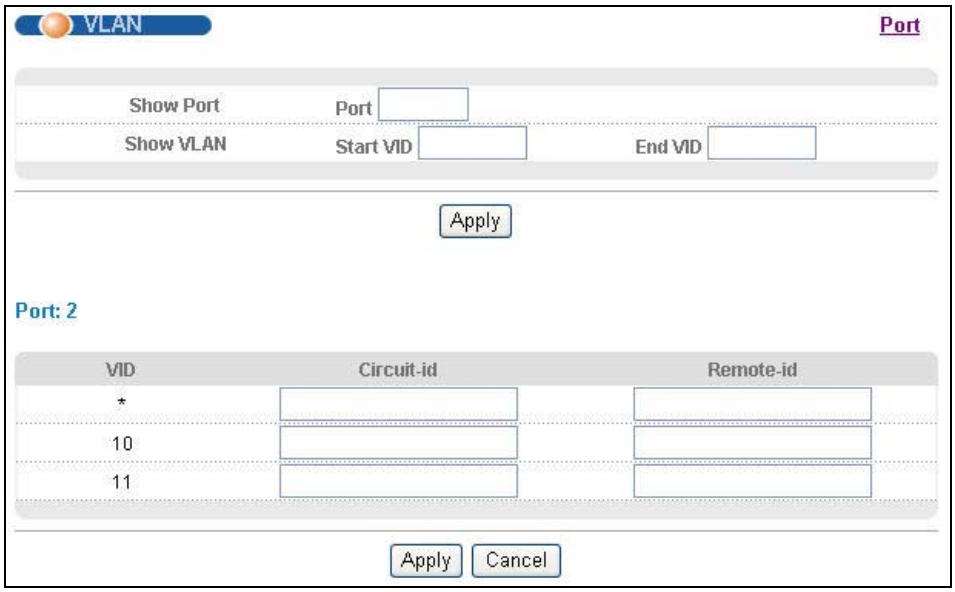
LABEL	DESCRIPTION
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Server Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are uplink ports connected to PPPoE servers. • If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports. • If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s). Untrusted ports are downlink ports connected to subscribers. • If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s). • The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. If you do not specify a string here or in the **Remote-id** field for a VLAN on a port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has the highest priority.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28.3.2 PPPoE IA Per-Port Per-VLAN

Use this screen to configure PPPoE IA settings that apply to a specific VLAN on a port.

Click the **VLAN** link in the **Intermediate Agent > Port** screen to display the screen as shown.

Figure 145 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN



The following table describes the labels in this screen.

Table 88 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

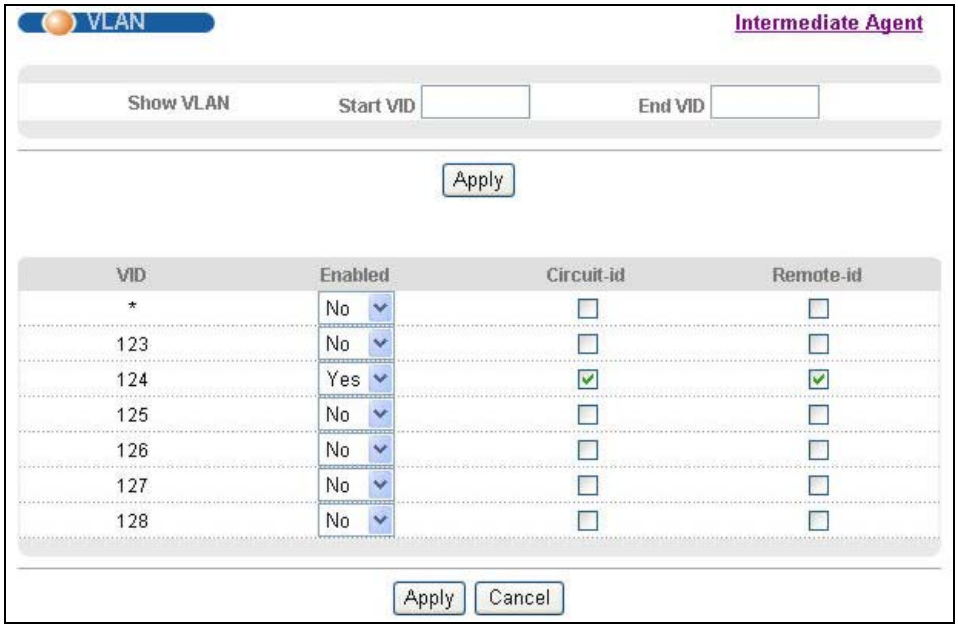
LABEL	DESCRIPTION
Show Port	Enter a port number to show the PPPoE Intermediate Agent settings for the specified VLAN(s) on the port.
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
Port	This field displays the port number specified above.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure here has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for this VLAN on the specified port. Spaces are allowed. If you do not specify a string here or in the **Remote-id** field for a specific port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure here has the highest priority.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28.3.3 PPPoE IA for VLAN

Use this screen to set whether the PPPoE Intermediate Agent is enabled on a VLAN and whether the Switch appends the Circuit ID and/or Remote ID to PPPoE discovery packets from a specific VLAN.

Click the **VLAN** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 146 Advanced Application > PPPoE > Intermediate Agent > VLAN



The following table describes the labels in this screen.

Table 89 Advanced Application > PPPoE > Intermediate Agent > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Enabled	Select this option to turn on the PPPoE Intermediate Agent on a VLAN.
Circuit-id	Select this option to make the Circuit ID settings for a specific VLAN take effect.
Remote-id	Select this option to make the Remote ID settings for a specific VLAN take effect.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29

Error Disable

29.1 Overview

This chapter shows you how to configure the rate limit for control packets on a port, and set the Switch to take an action (such as to shut down a port or stop sending packets) on a port when the Switch detects a pre-configured error. It also shows you how to configure the Switch to automatically undo the action after the error is gone.

29.1.1 What You Can Do

- Use the **Errdisable** screen (Section 29.2 on page 232) to display the main Error Disable screen.
- Use the **CPU Protection** screen (Section 29.3 on page 232) to to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port.
- Use the **Errdisable Detect** screen (Section 29.4 on page 233) to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
- Use the **Errdisable Recovery** screen (Section 29.5 on page 234) to set the Switch to automatically undo an action after the error is gone.

29.1.2 What You Need to Know

Read on for concepts on Error Disable that can help you configure the screen in this chapter.

29.1.2.1 CPU Protection

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other network(s). You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

29.1.2.2 Error-Disable Recovery

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the port(s) loop back to the Switch, the Switch can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator or the commands. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

29.2 The Error Disable Screen

Use this screen to configure error disable related settings. Click **Advanced Application > Errdisable** in the navigation panel to open the following screen.

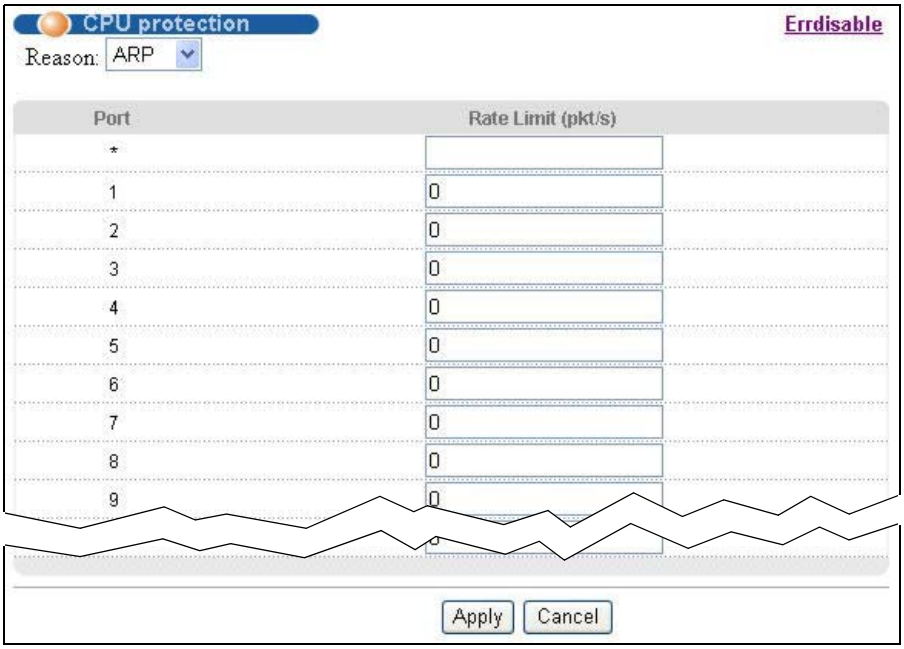
Figure 147 Advanced Application > Errdisable

29.3 CPU Protection Configuration

Use this screen to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port. Click the **Click Here** link next to **CPU protection** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Note: After you configure this screen, make sure you also enable error detection for the specific control packets in the **Advanced Application** > **Errdisable** > **Errdisable Detect** screen.

Figure 148 Advanced Application > Errdisable > CPU protection



The following table describes the labels in this screen.

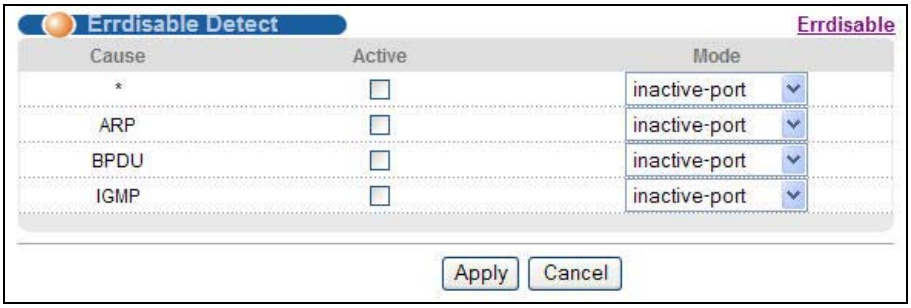
Table 90 Advanced Application > Errdisable > CPU protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. **0** means no rate limit. You can configure the action that the Switch takes when the limit is exceeded. See Section 29.4 on page 233 for detailed information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29.4 Error-Disable Detect Configuration

Use this screen to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded. Click the **Click Here** link next to **Errdisable Detect** link in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 149 Advanced Application > Errdisable > Errdisable Detect



The following table describes the labels in this screen.

Table 91 Advanced Application > Errdisable > Errdisable Detect

LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.

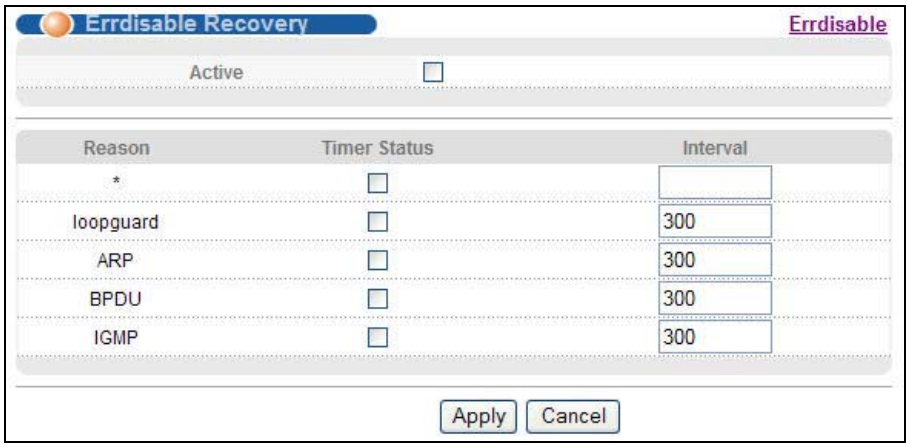
Table 91 Advanced Application > Errdisable > Errdisable Detect (continued)

LABEL	DESCRIPTION
Mode	Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the **Advanced Application > Errdisable > CPU protection** screen. • **inactive-port** - The Switch disables the port on which the control packets are received. • **inactive-reason** - The Switch bypasses the processing of the specified control packets (such as ARP or IGMP packets), or drops all the specified control packets (such as BPDU) on the port. • **rate-limitation** - The Switch drops the additional control packets the port has to handle in every one second.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29.5 Error-Disable Recovery Configuration

Use this screen to configure the Switch to automatically undo an action after the error is gone. Click the **Click Here** link next to **Errdisable Recovery** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 150 Advanced Application > Errdisable > Errdisable Recovery



The following table describes the labels in this screen.

Table 92 Advanced Application > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Select this option to turn on the error-disable recovery function on the Switch.
Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.

Table 92 Advanced Application > Errdisable > Errdisable Recovery (continued)

LABEL	DESCRIPTION
Timer Status	Select this option to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30

Static Route

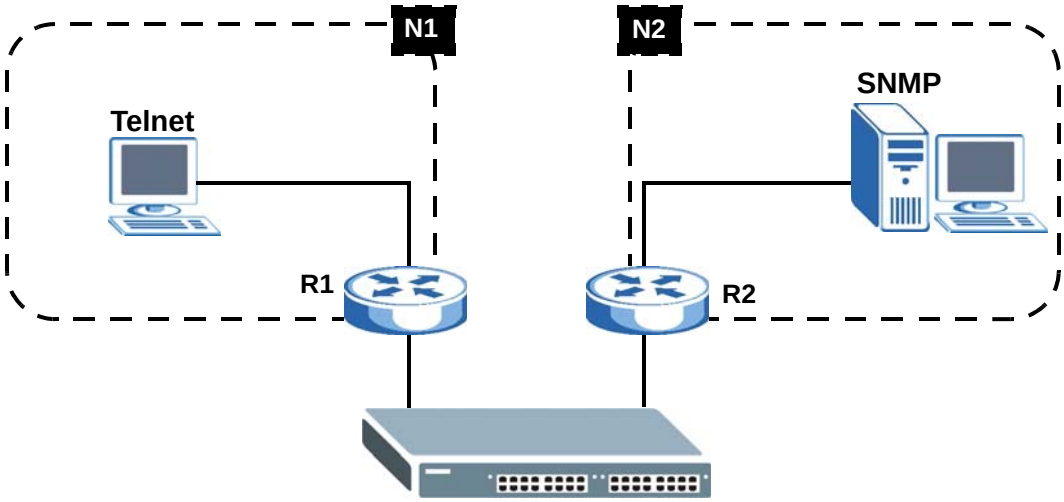
30.1 Overview

This chapter shows you how to configure static routes.

The Switch uses IP for communication with management computers, for example using HTTP, Telnet, SSH, or SNMP. Use IP static routes to have the Switch respond to remote management stations that are not reachable through the default gateway. The Switch can also use static routes to send data to a server or device that is not reachable through the default gateway, for example when sending SNMP traps or using ping to test IP connectivity.

This figure shows a **Telnet** session coming in from network **N1**. The Switch sends reply traffic to default gateway **R1** which routes it back to the manager's computer. The Switch needs a static route to tell it to use router **R2** to send traffic to an SNMP trap server on network **N2**.

Figure 151 Static Routing Overview



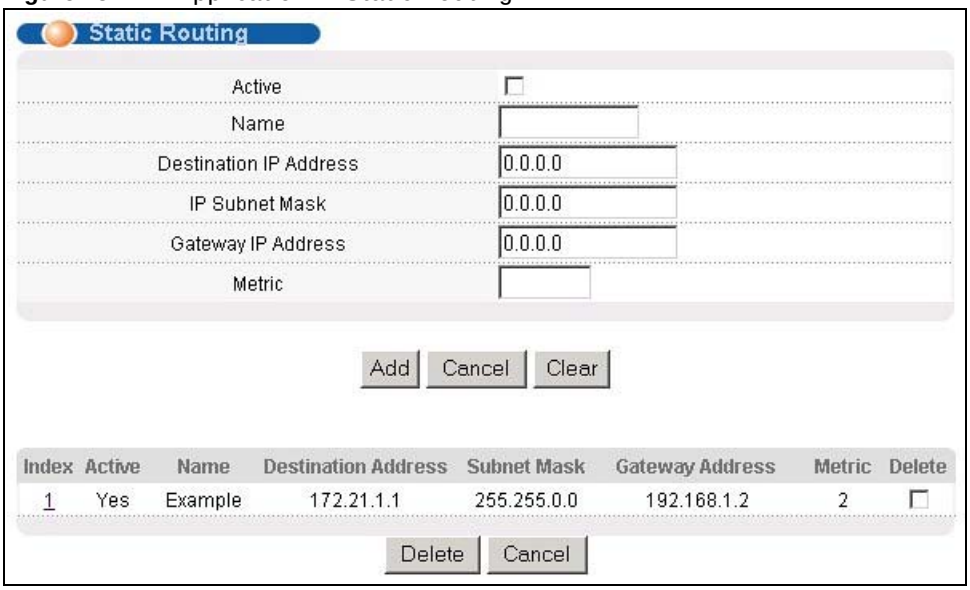
30.1.1 What You Can Do

Use the **Static Routing** screen (Section 30.2 on page 238) to activate/deactivate this static route.

30.2 Configuring Static Routing

Click **IP Application > Static Routing** in the navigation panel to display the screen as shown.

Figure 152 IP Application > Static Routing



The following table describes the related labels you use to create a static route.

Table 93 IP Application > Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
IP Subnet Mask	Enter the subnet mask for this destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to insert a new static route to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the above fields to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **NO** when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purposes only.

Table 93 IP Application > Static Routing (continued)

LABEL	DESCRIPTION
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

31

Differentiated Services

31.1 Overview

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

31.1.1 What You Can Do

- Use the **DiffServ** screen (Section 31.2 on page 241) to activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the Switch.
- Use the **DSCP** screen (Section 31.3.1 on page 242) to change the DSCP-IEEE 802.1p mapping.

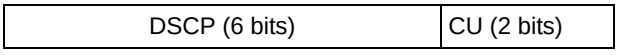
31.1.2 What You Need to Know

Read on for concepts on Differentiated Services that can help you configure the screens in this chapter.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

Figure 153 DiffServ: Differentiated Service Field



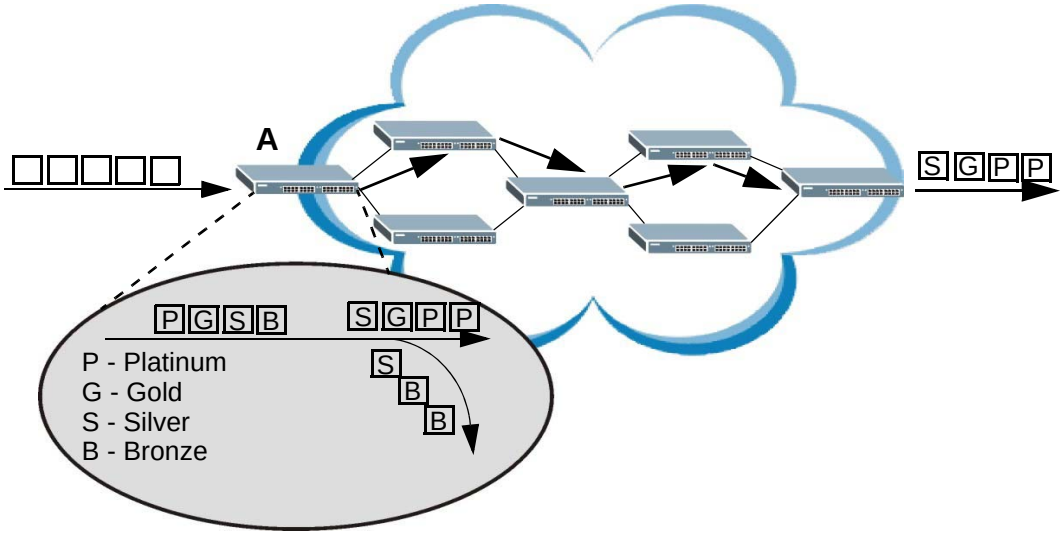
DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in Figure 154) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum**, **Gold**, **Silver**, **Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 154 DiffServ Network

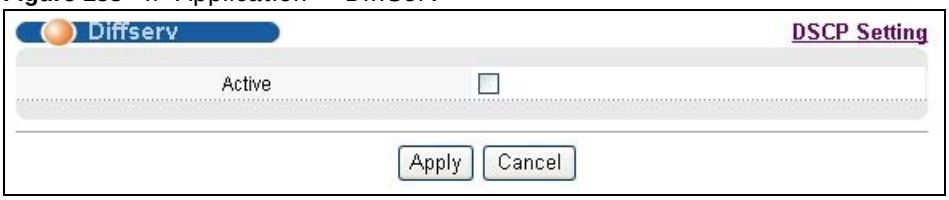


31.2 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the Switch.

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

Figure 155 IP Application > DiffServ



The following table describes the labels in this screen.

Table 94 IP Application > DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

31.3 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

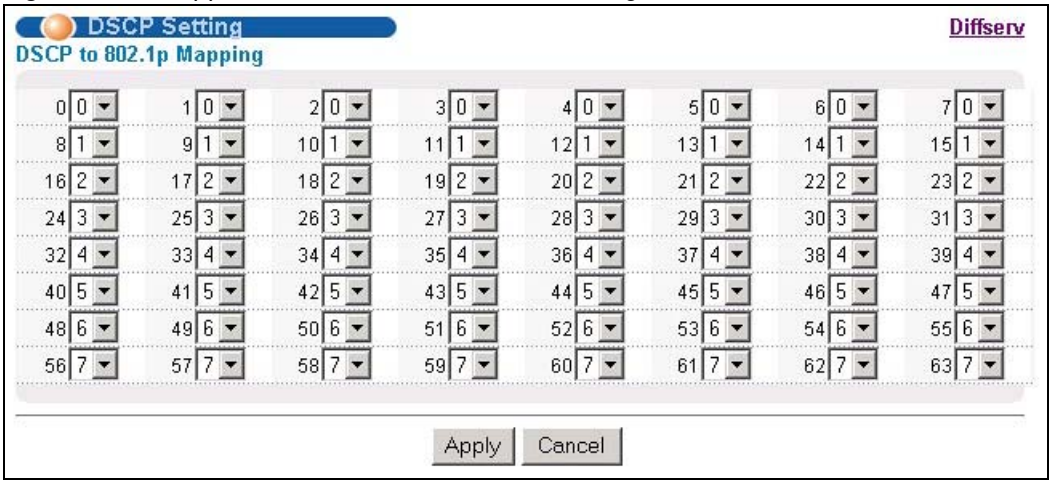
Table 95 Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

31.3.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 156 IP Application > DiffServ > DSCP Setting



The following table describes the labels in this screen.

Table 96 IP Application > DiffServ > DSCP Setting

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

32

DHCP

32.1 DHCP Overview

This chapter shows you how to configure the DHCP feature.

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. If you configure the Switch as a DHCP relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don't configure the Switch as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

32.1.1 What You Can Do

- Use the **DHCP Status** screen (Section 32.2 on page 245) to display the relay mode.
- Use the **DHCP Relay** screen (Section 32.3 on page 246) to enable and configure global DHCP relay.
- Use the **VLAN Setting** screen (Section 32.4 on page 247) to configure your DHCP settings based on the VLAN domain of the DHCP clients.

32.1.2 What You Need to Know

Read on for concepts on DHCP that can help you configure the screens in this chapter.

DHCP Modes

If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

DHCP Configuration Options

The DHCP configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global**: The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN**: The Switch is configured on a VLAN by VLAN basis. The Switch can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

DHCP Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field to the **Option 82** field. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Settings** > **General Setup**.

The following describes the DHCP relay information that the Switch sends to the DHCP server:

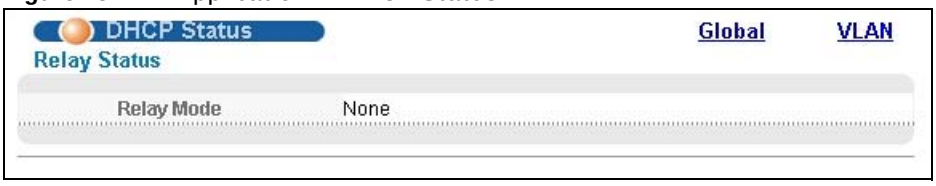
Table 97 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 64 bytes) This optional, read-only field is set according to system name set in **Basic Settings > General Setup.**

32.2 DHCP Status

Click **IP Application** > **DHCP** in the navigation panel. The **DHCP Status** screen displays.

Figure 157 IP Application > DHCP Status



The following table describes the labels in this screen.

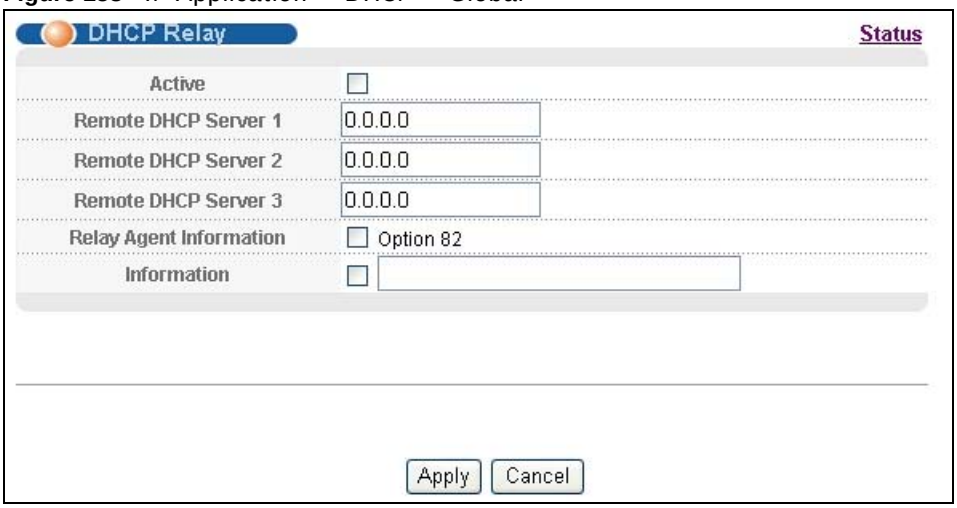
Table 98 IP Application > DHCP

LABEL	DESCRIPTION
Relay Mode	This field displays: • **None**: if the Switch is not configured as a DHCP relay agent. • **Global**: if the Switch is configured as a DHCP relay agent only. • **VLAN**: followed by a VLAN ID if it is configured as a relay agent for specific VLAN(s).

32.3 Configuring DHCP Global Relay

Configure global DHCP relay in the **DHCP Relay** screen. Click **IP Application > DHCP** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 158 IP Application > DHCP > Global



The following table describes the labels in this screen.

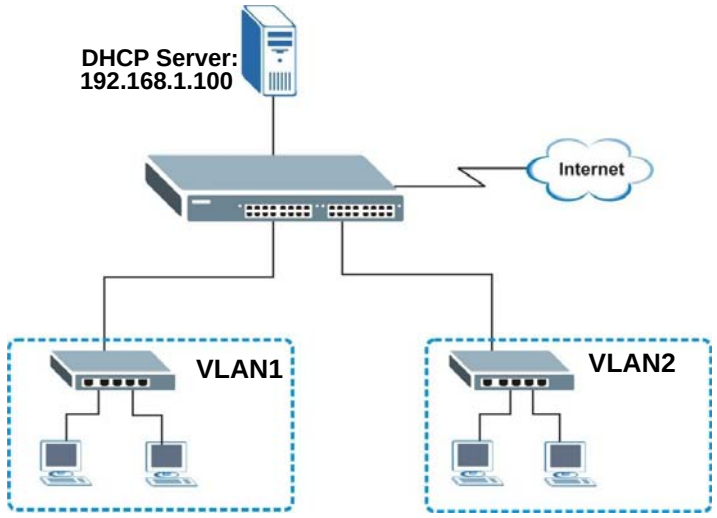
Table 99 IP Application > DHCP > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

32.3.1 Global DHCP Relay Configuration Example

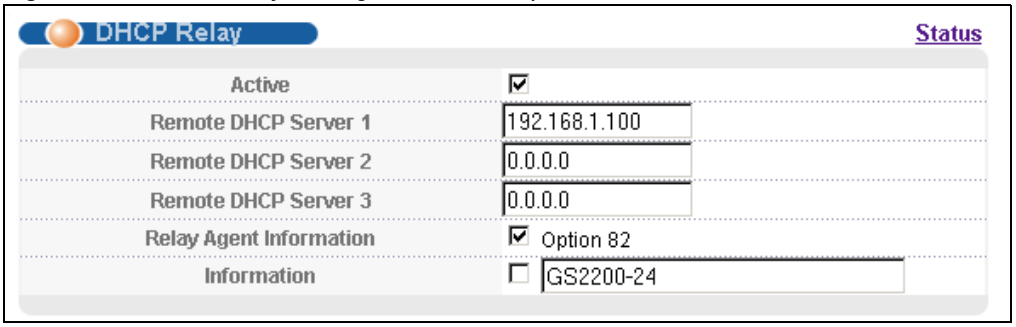
The following figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 159 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 160 DHCP Relay Configuration Example



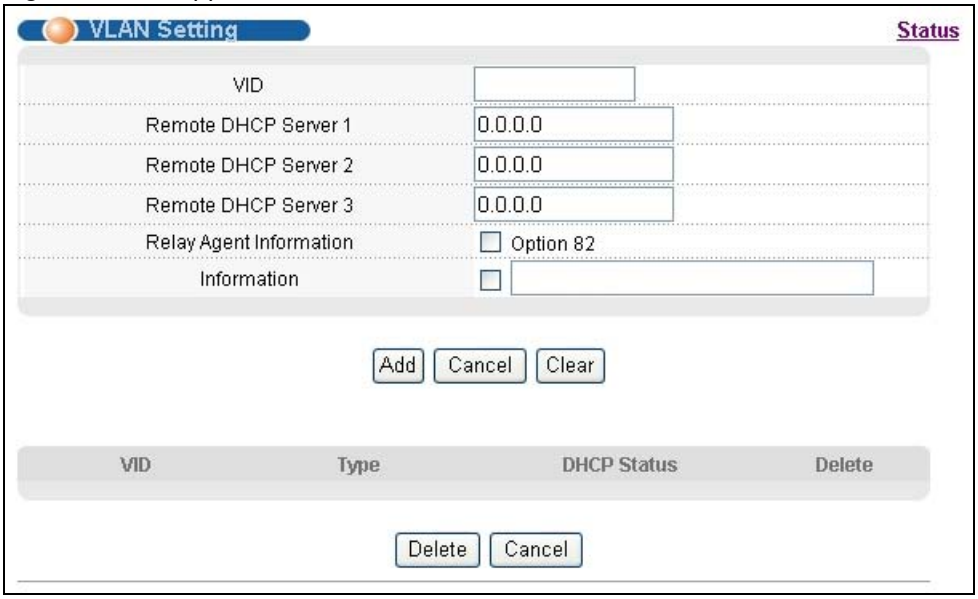
32.4 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application** > **DHCP** in the navigation panel, then click the **VLAN** link In the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch.

See Section 8.6 on page 72 for information on how to set up management IP addresses for VLANs.

Figure 161 IP Application > DHCP > VLAN



The following table describes the labels in this screen.

Table 100 IP Application > DHCP > VLAN

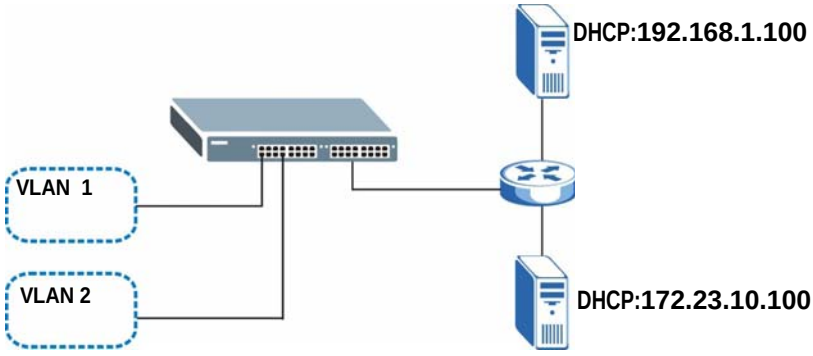
LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click this to clear the fields above.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays the DHCP mode (**Relay**).
DHCP Status	For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click **Delete** to remove them.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

32.4.1 Example: DHCP Relay for Two VLANs

The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from

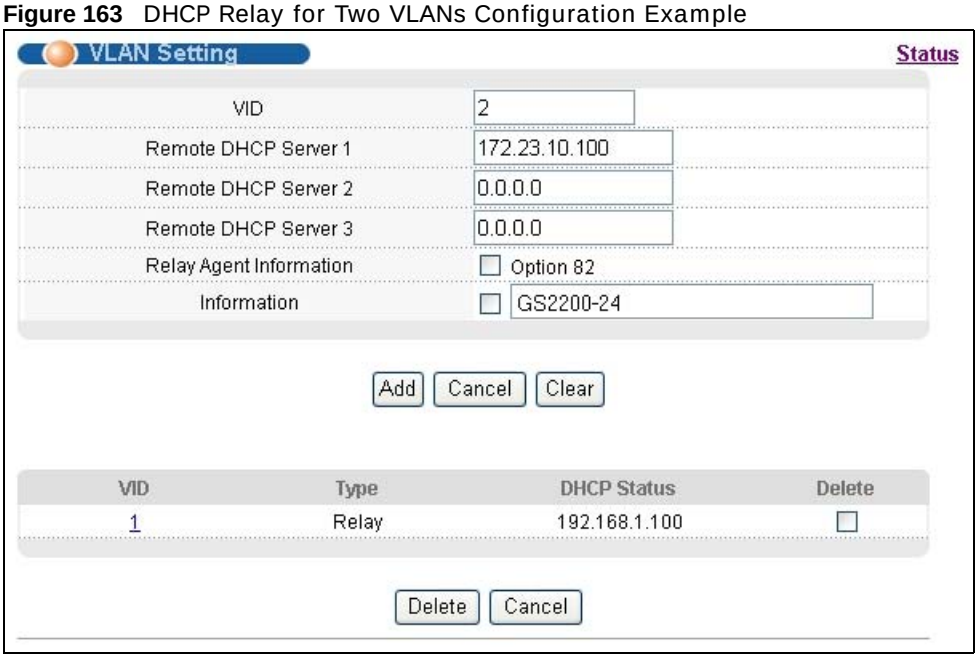
the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.23.10.100.

Figure 162 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 163 DHCP Relay for Two VLANs Configuration Example



33

ARP Learning

33.1 ARP Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

33.1.1 What You Can Do

Use the **ARP Learning** screen (Section 33.2 on page 252) to configure ARP learning mode on a per-port basis.

33.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

33.1.2.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

33.1.2.2 ARP Learning Mode

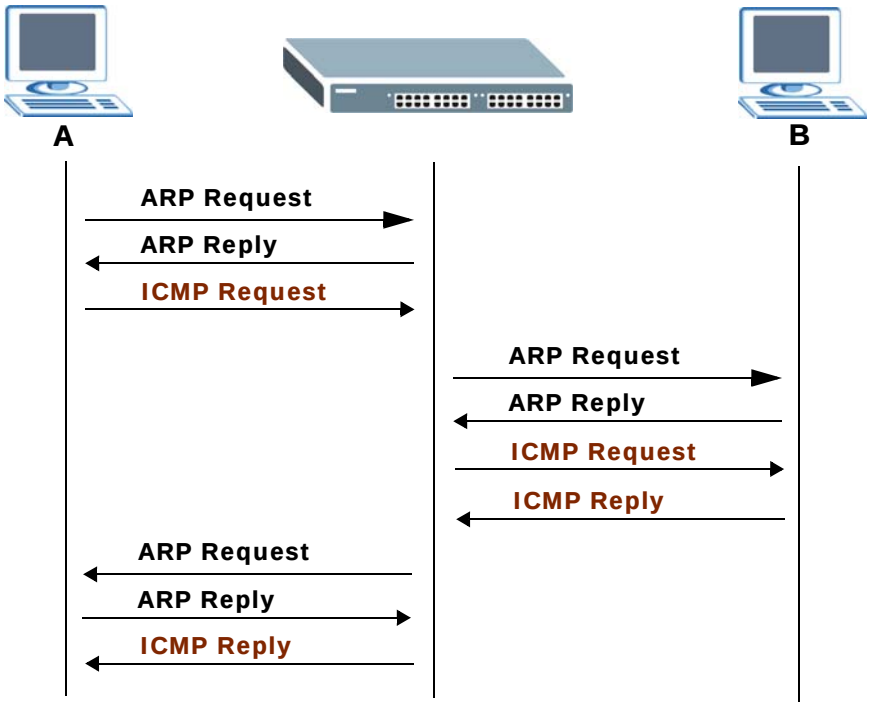
The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

ARP-Reply

By default, the Switch is in ARP-Reply learning mode and updates the ARP table only with the ARP replies to the ARP requests sent by the Switch. This can help prevent ARP spoofing.

In the following example, the Switch does not have IP address and MAC address mapping information for hosts **A** and **B** in its ARP table, and host **A** wants to ping host **B**. Host **A** sends an

ARP request to the Switch and then sends an ICMP request after getting the ARP reply from the Switch. The Switch finds no matched entry for host **B** in the ARP table and broadcasts the ARP request to all the devices on the LAN. When the Switch receives the ARP reply from host **B**, it updates its ARP table and also forwards host **A**'s ICMP request to host **B**. After the Switch gets the ICMP reply from host **B**, it sends out an ARP request to get host **A**'s MAC address and updates the ARP table with host **A**'s ARP reply. The Switch then can forward host **B**'s ICMP reply to host **A**.



Gratuitous-ARP

A gratuitous ARP is an ARP request in which both the source and destination IP address fields are set to the IP address of the device that sends this request and the destination MAC address field is set to the broadcast address. There will be no reply to a gratuitous ARP request.

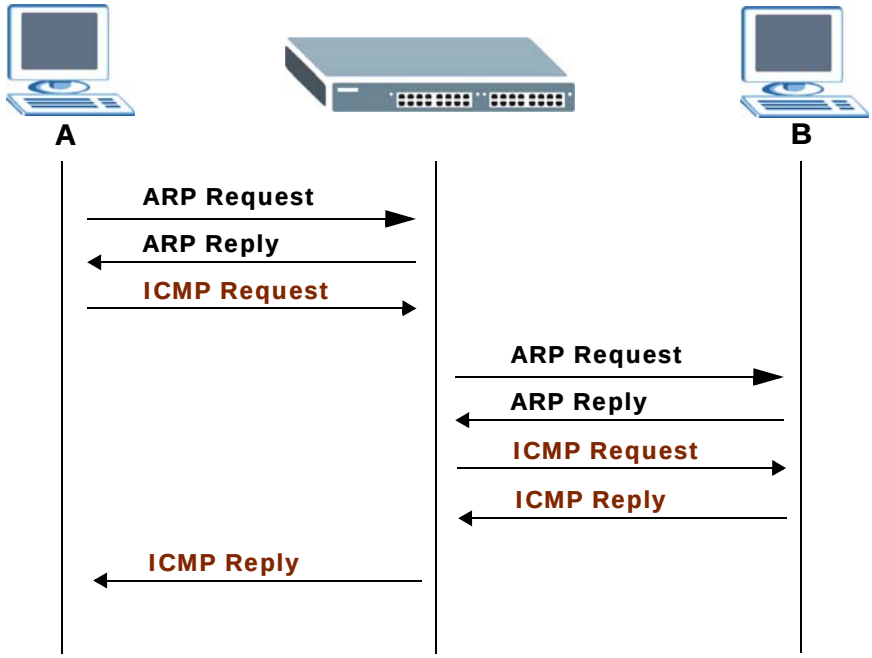
A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

In Gratuitous-ARP learning mode, the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request.

ARP-Request

When the Switch is in ARP-Request learning mode, it updates the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.

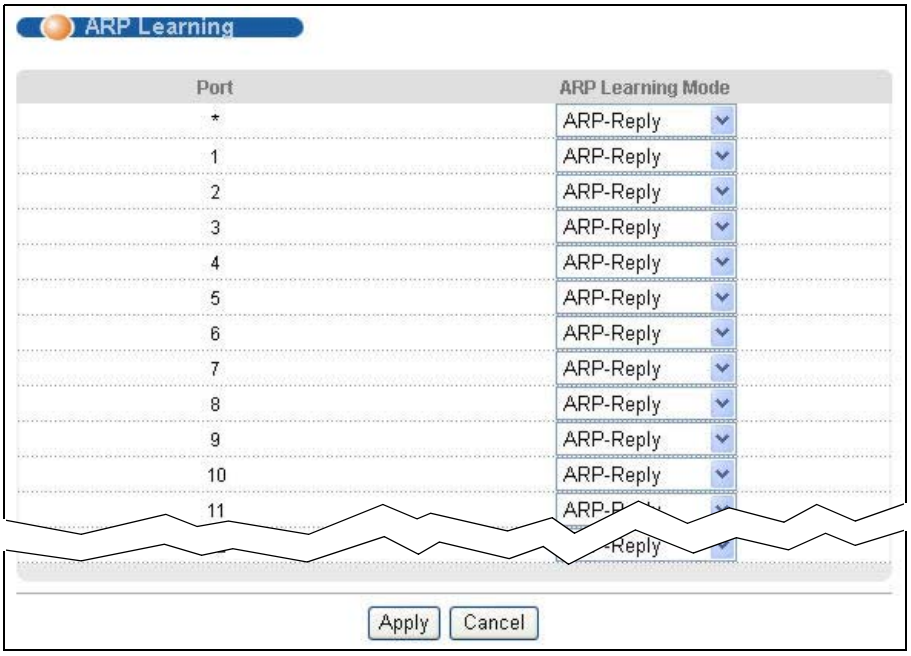
Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC address and ICMP reply.



33.2 Configuring ARP Learning

Click **IP Application** > **ARP Learning** in the navigation panel to display the screen as shown next.

Figure 164 IP Application > ARP Learning



The following table describes the labels in this screen.

Table 101 IP Application > ARP Learning

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
ARP Learning Mode	Select the ARP learning mode the Switch uses on the port. Select **ARP-Reply** to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select **Gratuitous-ARP** to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select **ARP-Request** to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34

Maintenance

34.1 Overview

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

34.1.1 What You Can Do

- Use the **Maintenance** screen (Section 34.2 on page 255) to return to the factory defaults, save the current configuration settings and restart the Switch.
- Use the **Firmware Upgrade** screen (Section 34.3 on page 257) to upload the latest firmware.
- Use the **Restore Configuration** screen (Section 34.4 on page 258) to upload a stored device configuration file.
- Use the **Backup Configuration** screen (Section 34.5 on page 258) to save your configurations for later use.

34.2 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management** > **Maintenance** in the navigation panel to open the following screen.

Figure 165 Management > Maintenance

The following table describes the labels in this screen.

Table 102 Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (**Configuration 1** or **Configuration 2**) is currently operating on the Switch.
Firmware Upgrade	Click **Click Here** to go to the **Firmware Upgrade** screen.

Table 102 Management > Maintenance (continued)

LABEL	DESCRIPTION
Restore Configuration	Click **Click Here** to go to the **Restore Configuration** screen.
Backup Configuration	Click **Click Here** to go to the **Backup Configuration** screen.
Load Factory Default	Click **Click Here** to reset the configuration to the factory default settings.
Save Configuration	Click **Config 1** to save the current configuration settings to **Configuration 1** on the Switch. Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.
Reboot System	Click **Config 1** to reboot the system and load **Configuration 1** on the Switch. Click **Config 2** to reboot the system and load **Configuration 2** on the Switch. Note: Make sure to click the **Save** button in any screen to save your settings to the current configuration on the Switch.

34.2.1 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Default** to clear all Switch configuration information you configured and return to the factory defaults.

2 Click **OK** to reset all Switch configurations to the factory defaults.

Figure 166 Load Factory Default: Start

3 In the web configurator, click the **Save** button in the top of the screen to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

34.2.2 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch.

Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

34.2.3 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the Switch.

1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 167 Reboot System: Confirmation

2 Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

34.3 Firmware Upgrade

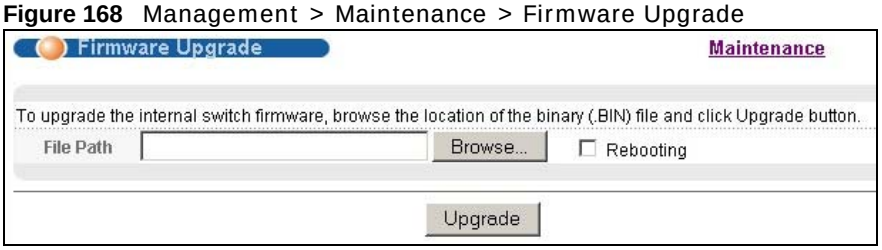
Use the following screen to upgrade your Switch to the latest firmware.

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

Click **Management** > **Maintenance** > **Firmware Upgrade** to view the screen as shown next.

Figure 168 Management > Maintenance > Firmware Upgrade



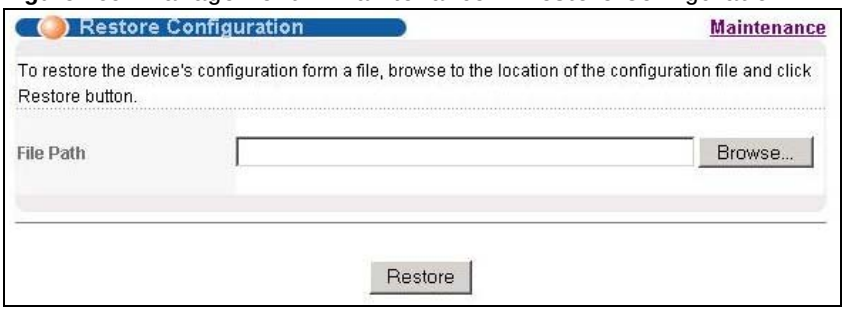
Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. Select the **Rebooting** checkbox if you want to reboot the Switch and apply the new firmware immediately. (Firmware upgrades are only applied after a reboot). Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

34.4 Restore a Configuration File

Use this screen to restore a previously saved configuration from your computer to the Switch.

Figure 169 Management > Maintenance > Restore Configuration



Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

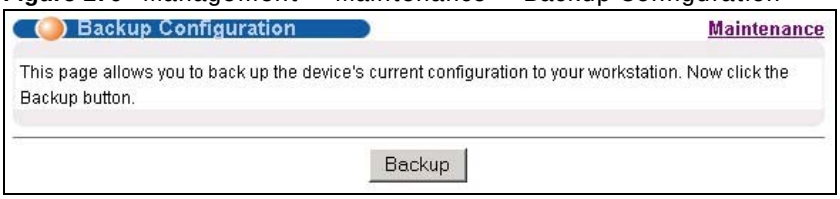
34.5 Backup a Configuration File

Use this screen to save and store your current device settings.

Backing up your Switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 170 Management > Maintenance > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Click **Backup**.

2 Click **Save** to display the **Save As** screen.

3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

34.6 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

34.6.1 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

34.6.2 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 103 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	*.cfg	This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

34.6.2.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

34.6.3 FTP Command Line Procedure

1. Launch the FTP client on your computer.
2. Enter open, followed by a space and the IP address of your Switch.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is “1234”).

5 Enter `bin` to set transfer mode to binary.

6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` transfers the firmware on your computer (firmware.bin) to the Switch and renames it to “ras”. Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the Switch and renames it to “config”. Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to “config.cfg”. See Table 103 on page 259 for more information on filename conventions.

7 Enter `quit` to exit the ftp prompt.

34.6.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

34.6.5 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

35

Access Control

35.1 Overview

This chapter describes how to control access to the Switch.

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five Web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 104 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to nine sessions		One session	Up to five accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the CLI Reference Guide for more information on disabling multi-login.

35.1.1 What You Can Do

- Use the **Access Control** screen (Section 35.2 on page 261) to display the main screen.
- Use the **SNMP** screen (Section 35.3 on page 262) to configure your SNMP settings.
- Use the **Trap Group** screen (Section 35.3.1 on page 264) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **User Information** screen (Section 35.3.2 on page 265) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **Logins** screens (Section 35.4 on page 266) to assign which users can access the Switch via web configurator at any one time.
- Use the **Service Access Control** screen (Section 35.5 on page 268) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen (Section 35.6 on page 268) to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

35.2 The Access Control Main Screen

Use this screen to display the main screen.

Click **Management** > **Access Control** in the navigation panel to display the main screen as shown.

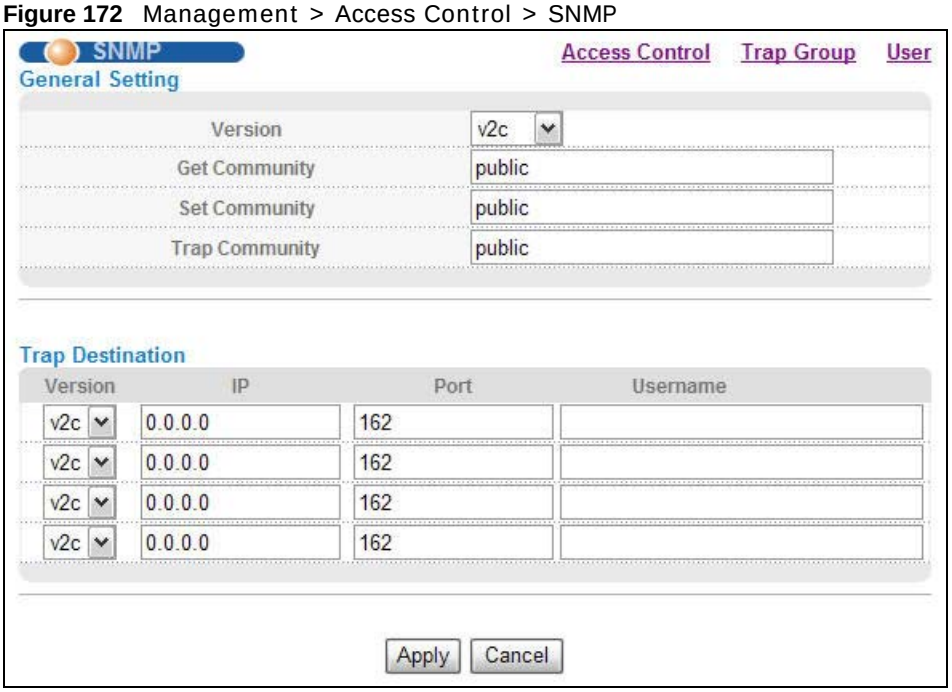
Figure 171 Management > Access Control

35.3 Configuring SNMP

Use this screen to configure your SNMP settings.

Click **Management** > **Access Control** > **SNMP** to view the screen as shown.

Figure 172 Management > Access Control > SNMP



The following table describes the labels in this screen.

Table 105 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (**v2c**), SNMP version 3 (**v3**) or both (**v3v2c**). Note: SNMP version 2c is backwards compatible with SNMP version 1.

Table 105 Management > Access Control > SNMP (continued)

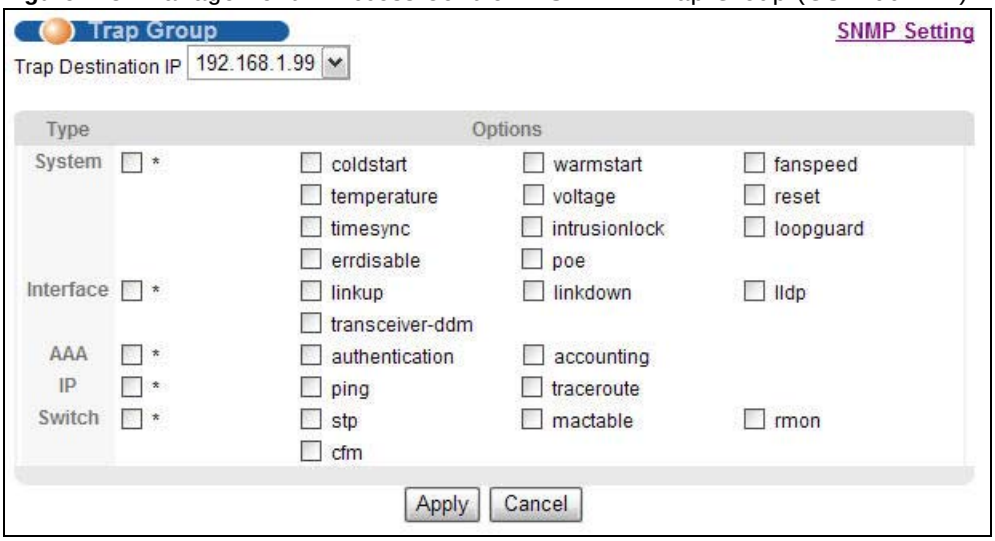
LABEL	DESCRIPTION
Get Community	Enter the **Get Community** string, which is the password for the incoming Get- and GetNext- requests from the management station. The **Get Community** string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the **Set Community** string, which is the password for the incoming Set- requests from the management station. The **Set Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the **Trap Community** string, which is the password sent with each trap to the SNMP manager. The **Trap Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. Note: This username must match an existing account on the Switch (configured in the **Management > Access Control > SNMP > User** screen).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.3.1 Configuring SNMP Trap Group

Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Click **Management** > **Access Control** > **SNMP** > **Trap Group** to view the screen as shown.

Figure 173 Management > Access Control > SNMP > Trap Group (GS2200-24P)



The following table describes the labels in this screen.

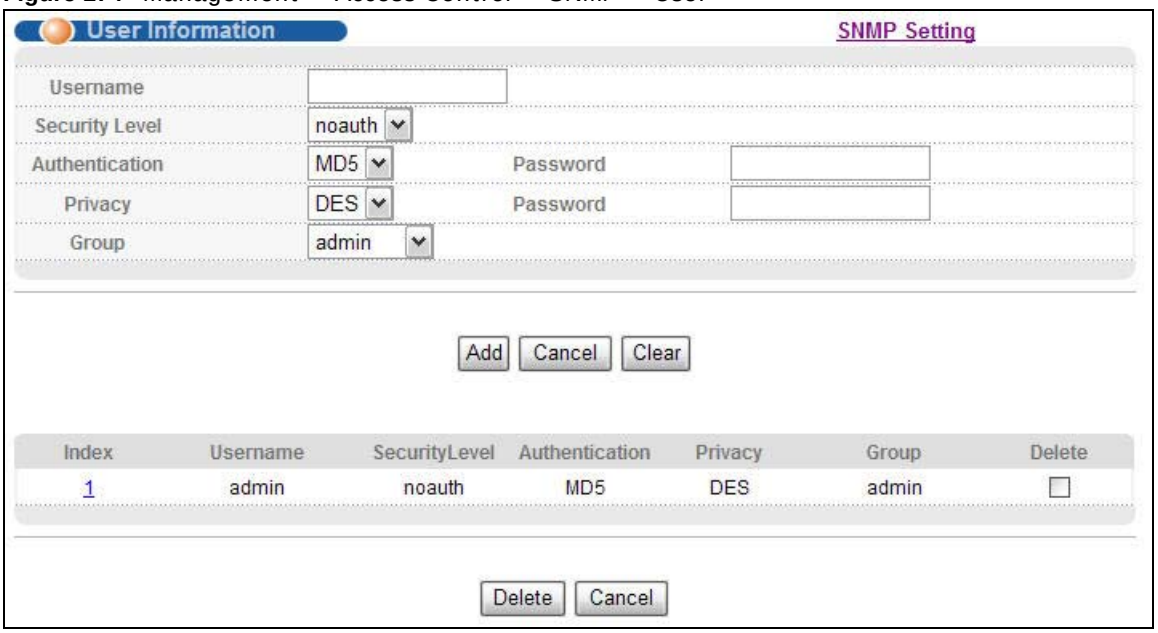
Table 106 Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the **SNMP Setting** screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See SNMP Traps on page 271 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories). Note: The **poe** and **fanspeed** options are only available in the GS2200-8HP and GS2200-24P.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.3.2 Configuring SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 174 Management > Access Control > SNMP > User



The following table describes the labels in this screen.

Table 107 Management > Access Control > SNMP > User

LABEL	DESCRIPTION
User Information	Note: Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.
Username	Specify the username of a login account on the Switch.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • **noauth** -to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • **auth** - to implement an authentication algorithm for SNMP messages sent by this user. • **priv** - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.
Authentication	Select an authentication algorithm. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Password	Enter the password of up to 32 ASCII characters for SNMP user authentication.

Table 107 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Password	Enter the password of up to 32 ASCII characters for encrypting SNMP packets.
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. **admin** - Members of this group can perform all types of system configuration, including the management of administrator accounts. **readwrite** - Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the Switch, except the user account and AAA configuration. **readonly** - Members of this group have read rights only, meaning the user can collect information from the Switch.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is a read-only number identifying a login account on the Switch. Click on an index number to view more details and edit an existing account.
Username	This field displays the username of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.4 Setting Up Login Accounts

Use this screen to assign which users can access the Switch via web configurator at any one time.

Up to five people (one administrator and four non-administrators) may access the Switch via web configurator at any one time.

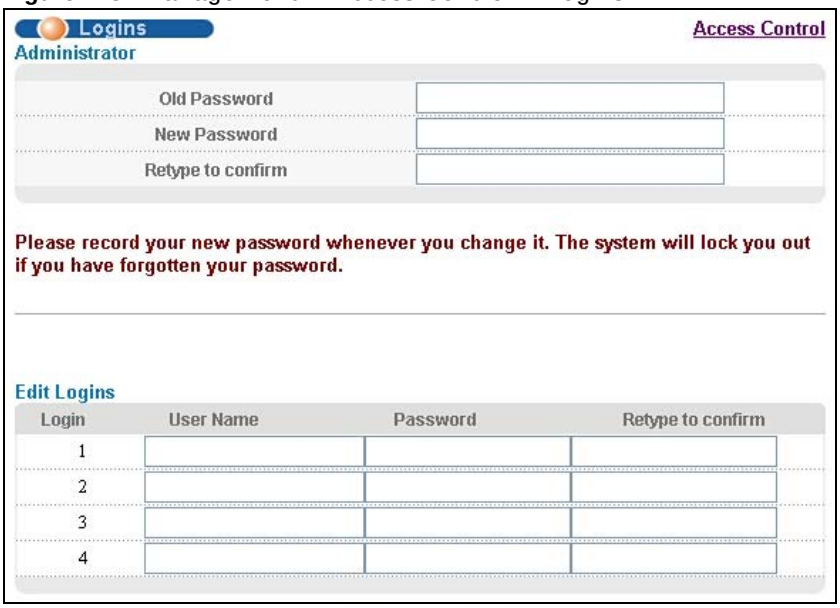
- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

Note: It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure Switch settings.

Click **Management** > **Access Control > Logins** to view the screen as shown next.

Figure 175 Management > Access Control > Logins



The following table describes the labels in this screen.

Table 108 Management > Access Control > Logins

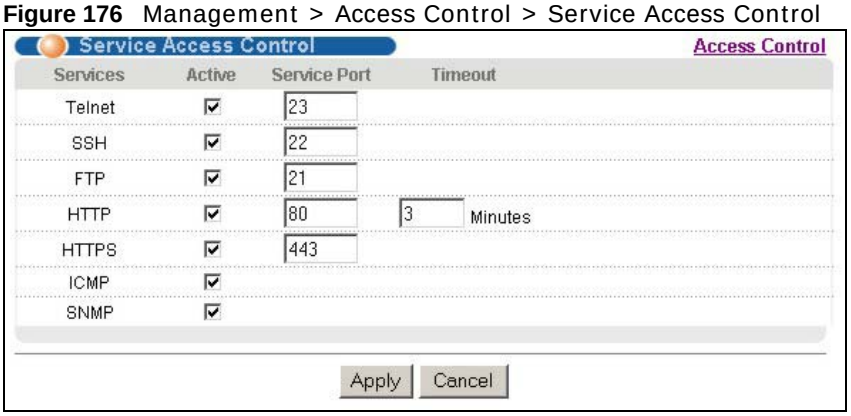
LABEL	DESCRIPTION
Administrator This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.	
Old Password	Type the existing system password (**1234** is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see the CLI Reference Guide.	
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35.5 Service Port Access Control

Use this screen to decide what services you may use to access the Switch.

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Management** > **Access Control > Service Access Control** to view the screen as shown.

Figure 176 Management > Access Control > Service Access Control



The following table describes the fields in this screen.

Table 109 Management > Access Control > Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Server Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

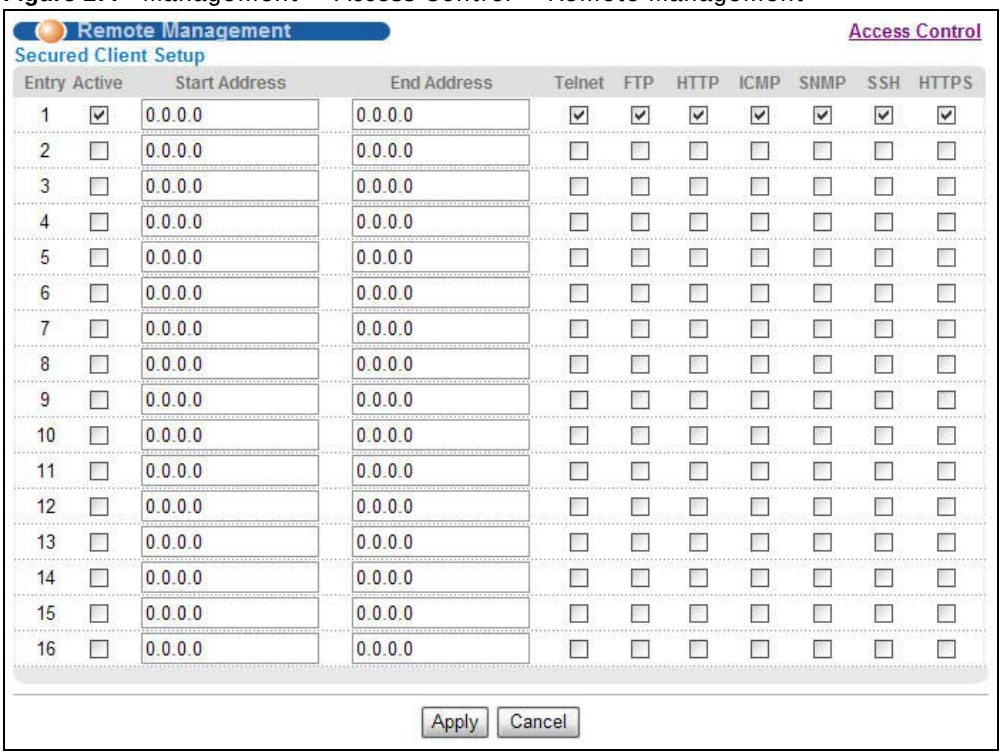
35.6 Remote Management

Use this screen to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

Click **Management** > **Access Control** > **Remote Management** to view the screen as shown next.

You can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

Figure 177 Management > Access Control > Remote Management



The following table describes the labels in this screen.

Table 110 Management > Access Control > Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this Switch. The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

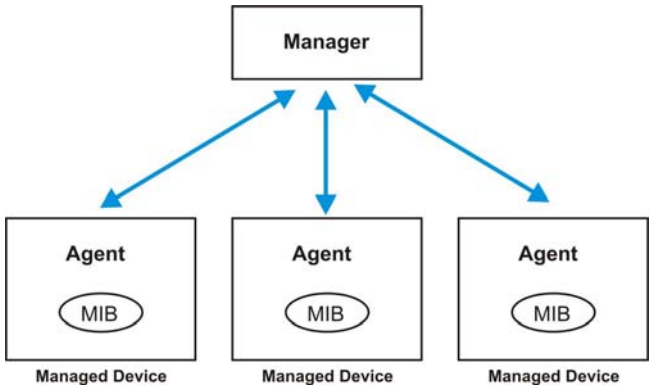
35.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

35.7.1 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version one (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 178 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the Switch). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 111 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.

Table 111 SNMP Commands

COMMAND	DESCRIPTION
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with "**1.3.6.1.4.1.890.1.5.8**" is defined in private MIBs. Otherwise, it is a standard MIB OID.

The OIDs beginning with "**1.3.6.1.4.1.890.1.5.8.55**" are specific to the GS2200-24. The OIDs beginning with "**1.3.6.1.4.1.890.1.5.8.56**" are specific to the GS2200-24P. The OIDs beginning with "**1.3.6.1.4.1.890.1.5.8.59**" are specific to the GS2200-8. The OIDs beginning with "**1.3.6.1.4.1.890.1.5.8.60**" are specific to the GS2200-8HP.

Table 112 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.

Table 112 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the temperature goes above or below the normal operating range.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.8.55.27.2.2 1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.59.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the temperature returns to the normal operating range.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the voltage goes above or below the normal operating range.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.8.55.27.2.2 1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.59.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the voltage returns to the normal operating range.
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the Switch automatically resets.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the Switch resets by an administrator through a management interface.
	RebootEvent	1.3.6.1.4.1.890.1.5.0.1	This trap is sent when the Switch reboots by an administrator through a management interface.
timesync	RTCNotUpdatedEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the Switch fails to get the time and date from a time server.
	RTCNotUpdatedEventClear	1.3.6.1.4.1.890.1.5.8.55.27.2.2 1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.59.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the Switch gets the time and date from a time server.

Table 112 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
intrusionlock	IntrusionLockEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when intrusion lock occurs on a port.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when loopguard shuts down a port.
errdisable	errdisableDetect	1.3.6.1.4.1.890.1.5.8.55.130.4.1 1.3.6.1.4.1.890.1.5.8.56.130.4.1 1.3.6.1.4.1.890.1.5.8.59.130.4.1 1.3.6.1.4.1.890.1.5.8.60.130.4.1	This trap is sent when an error is detected on a port, such as a loop occurs or the rate limit for specific control packets is exceeded.
	errdisableRecovery	1.3.6.1.4.1.890.1.5.8.55.130.4.2 1.3.6.1.4.1.890.1.5.8.56.130.4.2 1.3.6.1.4.1.890.1.5.8.59.130.4.2 1.3.6.1.4.1.890.1.5.8.60.130.4.2	This trap is sent when the Switch ceases the action taken on a port, such as shutting down the port or discarding packets on the port, after the specified recovery interval.
fanspeed	FanSpeedEventOn	1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the fan speed returns to the normal operating range.
poe	PwrPortFailedEventOn	1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the port is turned off to supply power due to overloading, over system buget, or short circuit.
	PwrPortFailedEventClear	1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the port returns to the normal state and has the ability to supply power.
	PsePwrFailedEventOn	1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the power supply of PoE failed. The trigger situation includes internal/external power supply failure, external fan speed failure, and external power has exceed normal temperature.
	PsePwrFailedEventClear	1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the power supply of PoE returns to the normal state.

Table 113 SNMP InterfaceTraps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
	LinkDownEventClear	1.3.6.1.4.1.890.1.5.8.55.27.2.2 1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.59.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
	LinkDownEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when the Ethernet link is down.
lldp	LLDPRemoteTopologyChange	1.0.8802.1.1.2.0.0.1	This trap is sent when the LLDP (Link Layer Discovery Protocol) remote topology changes.
transceiver-ddm	DDMIRxPowerEventOn DDMITemperatureEventOn DDMITxBiasEventOn DDMITxPowerEventOn DDMIVoltageEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when one of the device operating parameters (such as transceiver temperature, laser bias current, transmitted optical power, received optical power and transceiver supply voltage) is above or below a factory set normal range.
	DDMIRxPowerEventClear DDMITemperatureEventClear DDMITxBiasEventClear DDMITxPowerEventClear DDMIVoltageEventClear	1.3.6.1.4.1.890.1.5.8.55.27.2.2 1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.59.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when all device operating parameters return to the normal operating range.

Table 114 AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	AuthenticationFailureEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	RADIUSNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when there is no response message from the RADIUS server.
	RADIUSNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.55.27.2.2 1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.59.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the RADIUS server can be reached.
accounting	RADIUSAccNotNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when there is no response message from the RADIUS accounting server.
	RADIUSAccNotNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.55.27.2.2 1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.59.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when the RADIUS accounting server can be reached.

Table 115 SNMP IP Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRoutePathChange	1.3.6.1.2.1.81.0.1	This trap is sent when path to target has changed from a previously determined path.
	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.

Table 116 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	MRSTPNewRoot	1.3.6.1.4.1.890.1.5.8.55.36.2.1 1.3.6.1.4.1.890.1.5.8.56.36.2.1 1.3.6.1.4.1.890.1.5.8.59.36.2.1 1.3.6.1.4.1.890.1.5.8.60.36.2.1	This trap is sent when the MRSTP root switch changes.
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.8.55.107.70.1 1.3.6.1.4.1.890.1.5.8.56.107.70.1 1.3.6.1.4.1.890.1.5.8.59.107.70.1 1.3.6.1.4.1.890.1.5.8.60.107.70.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	MRSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.55.36.2.2 1.3.6.1.4.1.890.1.5.8.56.36.2.2 1.3.6.1.4.1.890.1.5.8.59.36.2.2 1.3.6.1.4.1.890.1.5.8.60.36.2.2	This trap is sent when the MRSTP topology changes.
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.55.107.70.2 1.3.6.1.4.1.890.1.5.8.56.107.70.2 1.3.6.1.4.1.890.1.5.8.59.107.70.2 1.3.6.1.4.1.890.1.5.8.60.107.70.2	This trap is sent when the MSTP root switch changes.
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.8.55.27.2.1 1.3.6.1.4.1.890.1.5.8.56.27.2.1 1.3.6.1.4.1.890.1.5.8.59.27.2.1 1.3.6.1.4.1.890.1.5.8.60.27.2.1	This trap is sent when more than 99% of the MAC table is used.
	MacTableFullEventClear	1.3.6.1.4.1.890.1.5.8.55.27.2.2 1.3.6.1.4.1.890.1.5.8.56.27.2.2 1.3.6.1.4.1.890.1.5.8.59.27.2.2 1.3.6.1.4.1.890.1.5.8.60.27.2.2	This trap is sent when less than 95% of the MAC table is used.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.
CFM	dot1agCfmFaultAlarm	1.3.111.2.802.1.1.8.0.1	The trap is sent when the Switch detects a connectivity fault.

35.7.2 SSH Overview

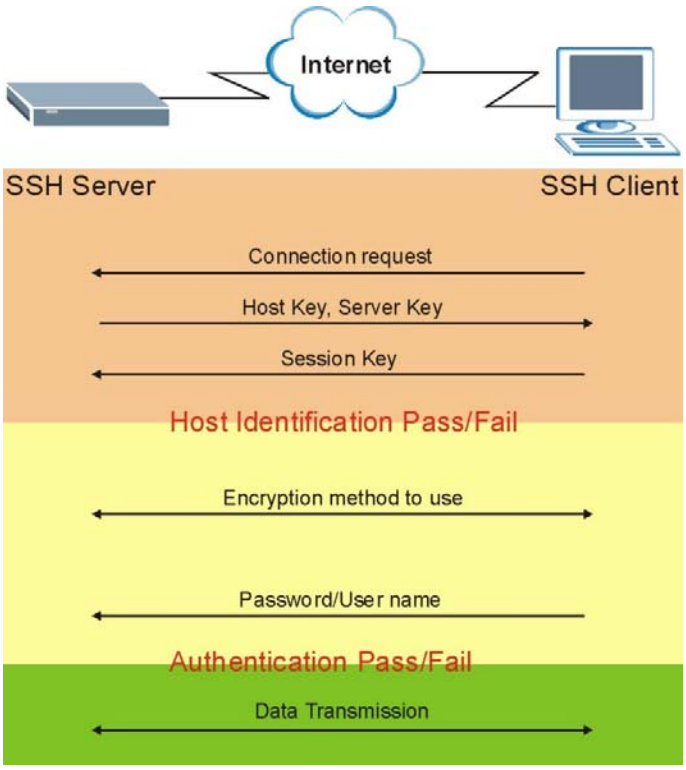
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 179 SSH Communication Example

35.7.2.1 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 180 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

35.7.2.2 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

35.7.2.3 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

35.7.3 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

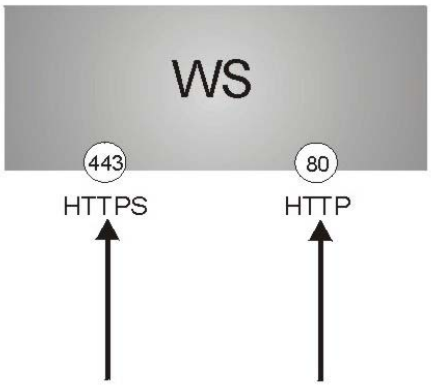
HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Switch.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).

2 HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 181 HTTPS Implementation



Note: If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

35.7.3.1 HTTPS Example

If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

Internet Explorer Warning Messages

Internet Explorer 6

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate.

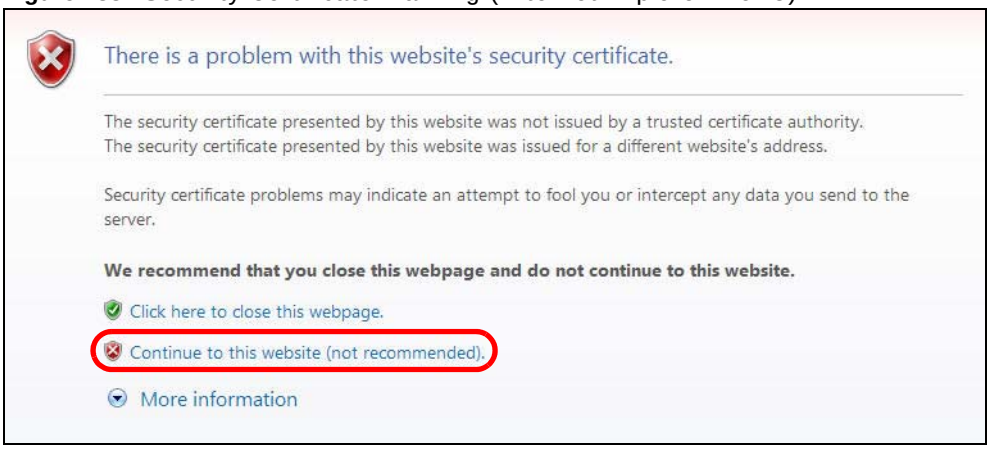
You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 182 Security Alert Dialog Box (Internet Explorer 6)

Internet Explorer 7 or 8

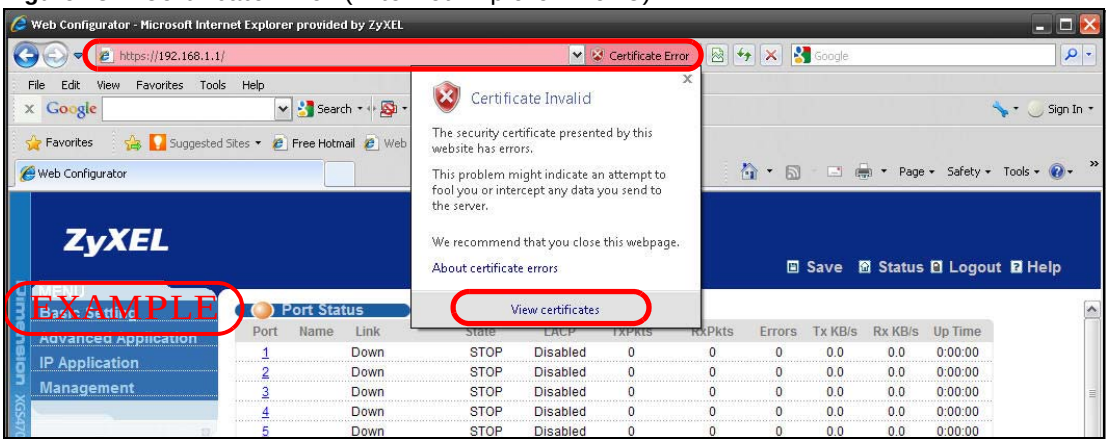
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the web configurator login screen.

Figure 183 Security Certificate Warning (Internet Explorer 7 or 8)



After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

Figure 184 Certificate Error (Internet Explorer 7 or 8)



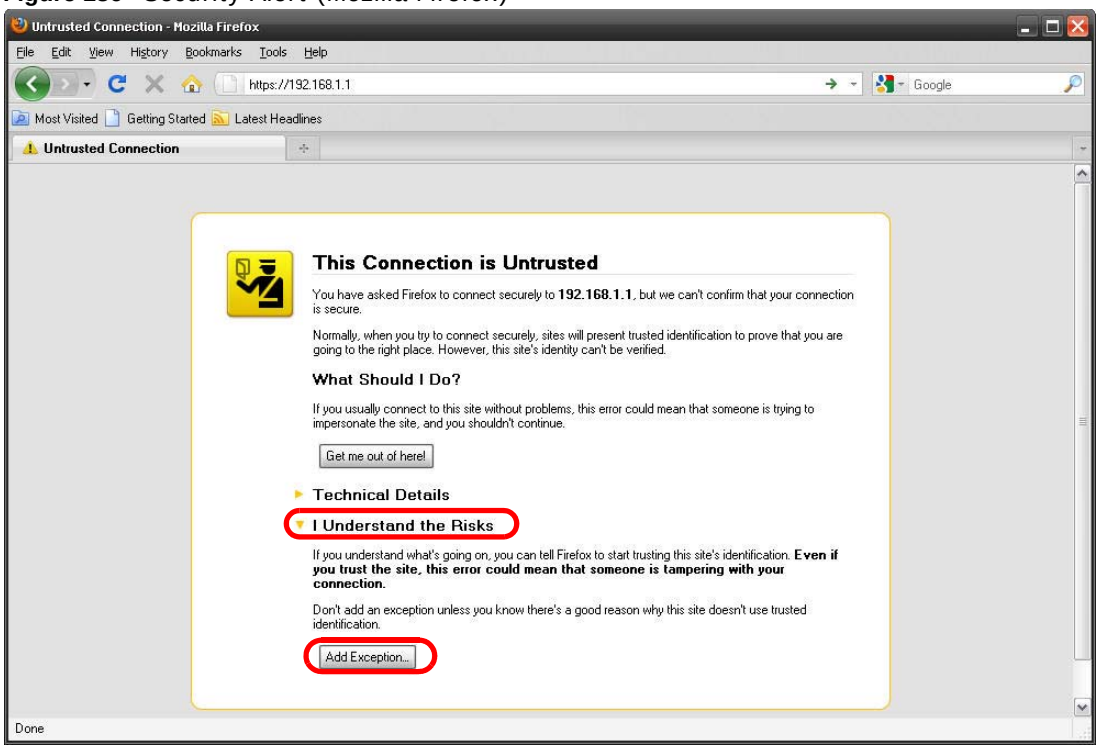
Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

Figure 185 Certificate (Internet Explorer 7 or 8)

Mozilla Firefox Warning Messages

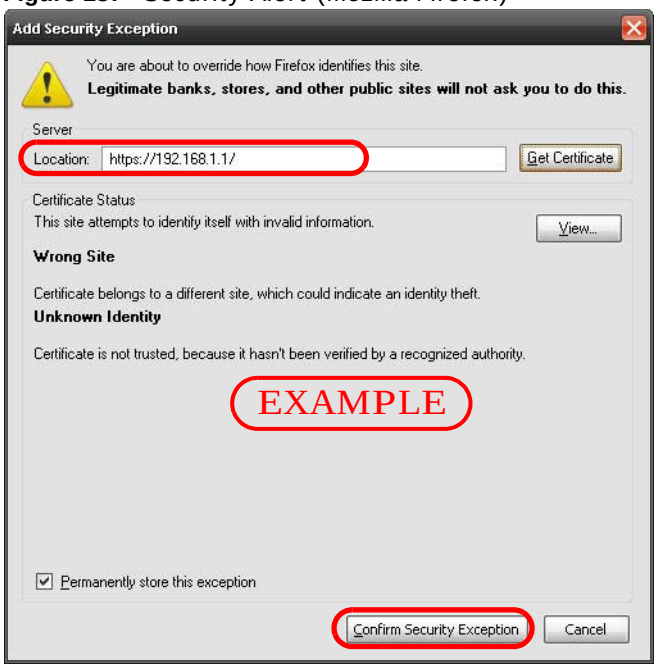
When you attempt to access the Switch HTTPS server, a **This Connection is Unstructed** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

Figure 186 Security Alert (Mozilla Firefox)



Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the web configurator login screen.

Figure 187 Security Alert (Mozilla Firefox)

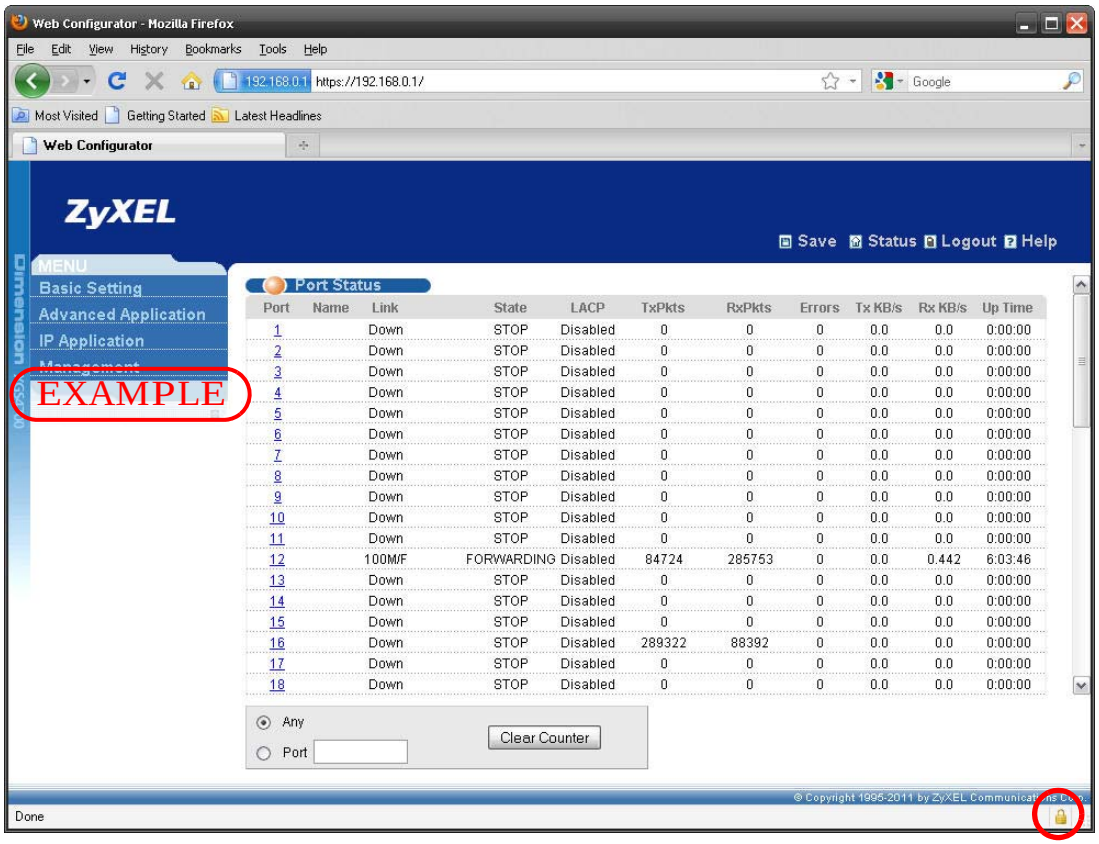


35.7.3.2 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar (in Internet Explorer 6 or

Mozilla Firefox) or next to the address bar (in Internet Explorer 7 or 8) denotes a secure connection.

Figure 188 Example: Lock Denoting a Secure Connection



36

Diagnostic

36.1 Overview

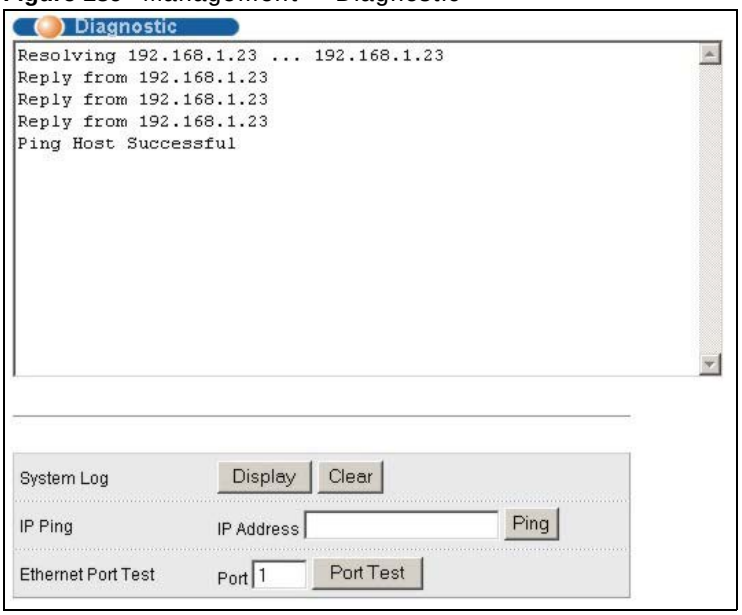
This chapter explains the **Diagnostic** screen.

Use the **Diagnostic** screen (Section 36.2 on page 285) to check system logs, ping IP addresses or perform port tests.

36.2 Diagnostic

Click **Management** > **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, ping IP addresses or perform port tests.

Figure 189 Management > Diagnostic



The following table describes the labels in this screen.

Table 117 Management > Diagnostic

LABEL	DESCRIPTION
System Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the syslog entry.

Table 117 Management > Diagnostic (continued)

LABEL	DESCRIPTION
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click **Ping** to have the Switch ping the IP address (in the field to the left).
Ethernet Port Test	Enter a port number and click **Port Test** to perform an internal loopback test.

37

Syslog

37.1 Overview

This chapter explains the syslog screens.

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 118 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

37.1.1 What You Can Do

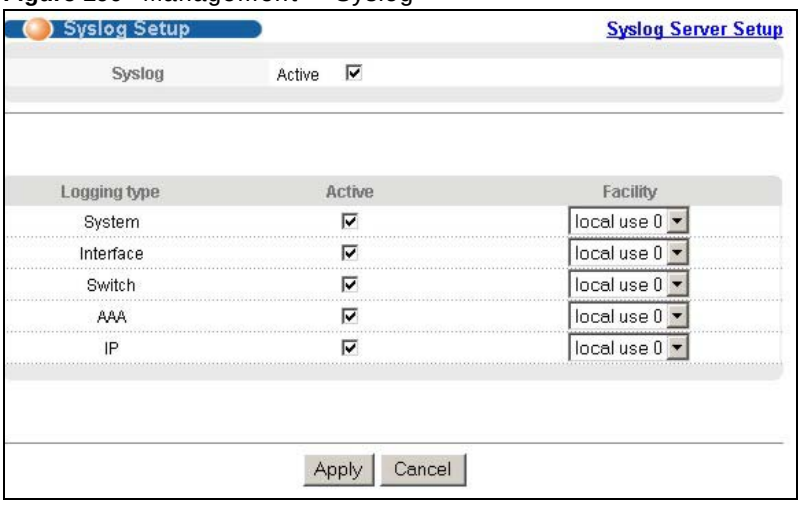
- Use the **Syslog Setup** screen (Section 37.2 on page 287) to configure the device's system logging settings.
- Use the **Syslog Server Setup** screen (Section 37.3 on page 289) to configure a list of external syslog servers.

37.2 Syslog Setup

Use this screen to configure the device's system logging settings.

Click **Management** > **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server.

Figure 190 Management > Syslog



The following table describes the labels in this screen.

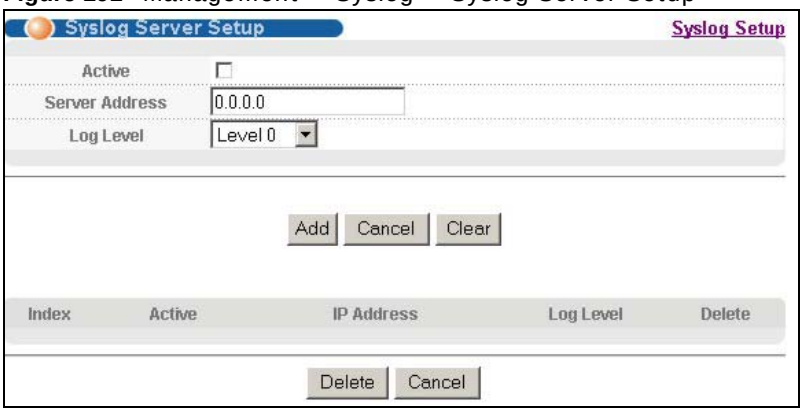
Table 119 Management > Syslog

LABEL	DESCRIPTION
Syslog	Select **Active** to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

37.3 Syslog Server Setup

Click **Management** > **Syslog** > **Syslog Server Setup** to view the screen as shown next. Use this screen to configure a list of external syslog servers.

Figure 191 Management > Syslog > Syslog Server Setup



The following table describes the labels in this screen.

Table 120 Management > Syslog > Syslog Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays **Yes** if the device is to send logs to the syslog server. **No** displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry.
Cancel	Click **Cancel** to begin configuring this screen afresh.

38

Cluster Management

38.1 Overview

This chapter introduces cluster management.

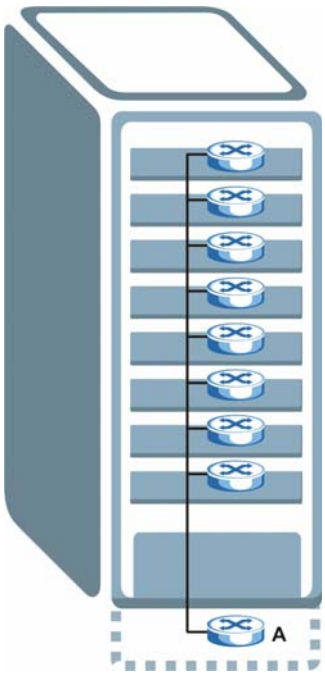
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 121 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 192 Clustering Application Example



38.1.1 What You Can Do

- Use the **Cluster Management** screen (Section 38.2 on page 291) to view the role of the Switch within the cluster and to access a cluster member switch's web configurator.
- Use the **Clustering Management Configuration** screen (Section 38.1 on page 290) to configure clustering management.

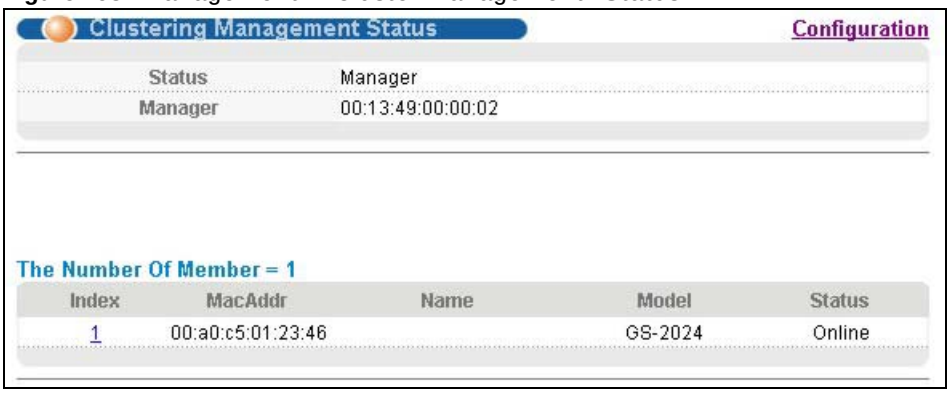
38.2 Cluster Management Status

Use this screen to view the role of the Switch within the cluster and to access a cluster member switch's web configurator.

Click **Management** > **Cluster Management** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 193 Management > Cluster Management: Status



The following table describes the labels in this screen.

Table 122 Management > Cluster Management: Status

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. **Manager** **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see Figure 195 on page 294).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.

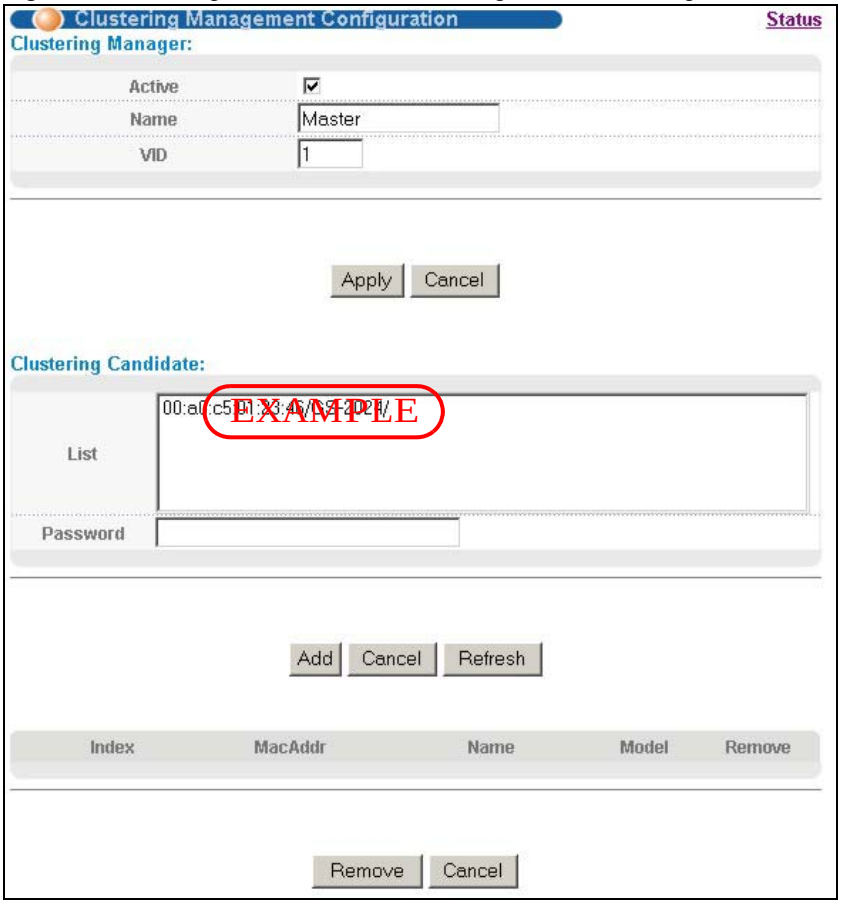
Table 122 Management > Cluster Management: Status (continued)

LABEL	DESCRIPTION
Model	This field displays the model name.
Status	This field displays: **Online** (the cluster member switch is accessible) **Error** (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

38.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Management** > **Cluster Management** > **Configuration** to display the next screen.

Figure 194 Management > Cluster Management > Configuration



The following table describes the labels in this screen.

Table 123 Management > Cluster Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select **Active** to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager.** You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to **802.1Q** VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the **Remove** button to remove a cluster member switch from the cluster.
Cancel	Click **Cancel** to begin configuring this screen afresh.

38.4 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

38.4.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 195 Cluster Management: Cluster Member Web Configurator Screen

38.4.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 196 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          393216 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 400BPN0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

Table 124 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Enter “admin”.
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch’s firmware and configuration file.
400BPN0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-01-23-46	This is the cluster member switch’s firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch’s configuration file name as seen in the cluster manager switch.

39

MAC Table

39.1 Overview

This chapter introduces the **MAC Table** screen.

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

39.1.1 What You Can Do

Use the **MAC Table** screen (Section 39.2 on page 297) to check whether the MAC address is dynamic or static.

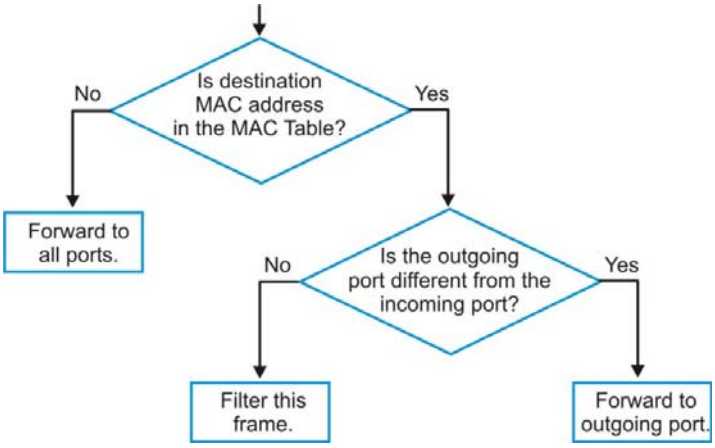
39.1.2 What You Need to Know

The Switch uses the MAC table to determine how to forward frames. See the following figure.

1. The Switch examines a received frame and learns the port on which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
   - If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
   - If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.

- If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 197 MAC Table Flowchart

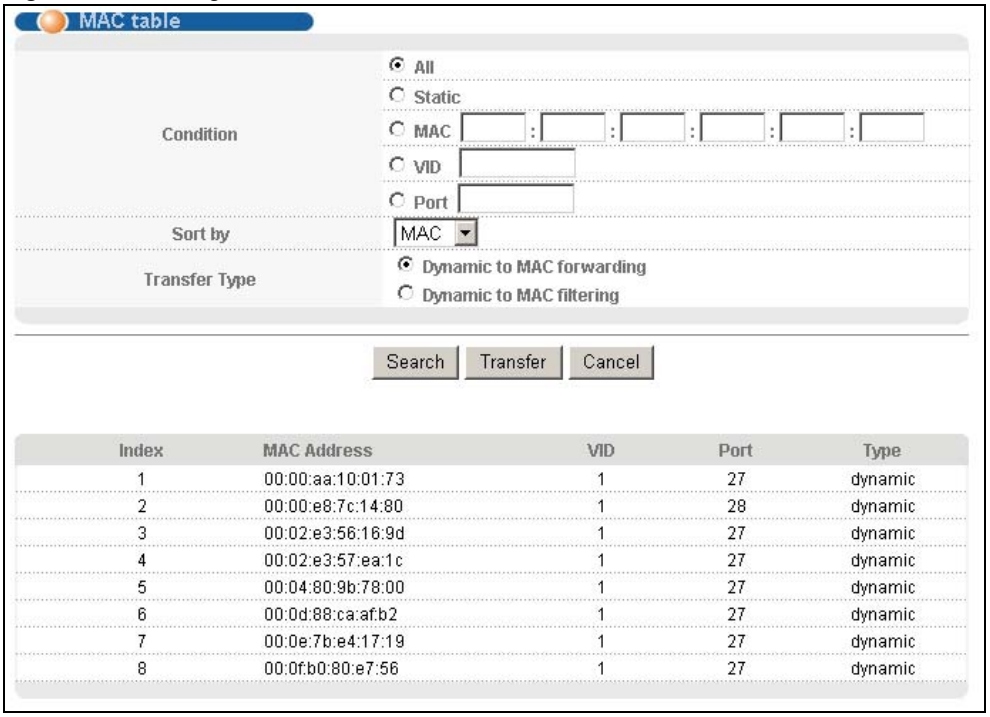


39.2 Viewing the MAC Table

Use this screen to check whether the MAC address is dynamic or static.

Click **Management** > **MAC Table** in the navigation panel to display the following screen.

Figure 198 Management > MAC Table



The following table describes the labels in this screen.

Table 125 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select one of the buttons and click **Search** to only display the data which matches the criteria you specified. Select **All** to display any entry in the MAC table of the Switch. Select **Static** to display the MAC entries manually configured on the Switch. Select **MAC** and enter a MAC address in the field provided to display a specified MAC entry. Select **VID** and enter a VLAN ID in the field provided to display the MAC entries belonging to the specified VLAN. Select **Port** and enter a port number in the field provided to display the MAC addresses which are forwarded on the specified port.
Sort by	Define how the Switch displays and arranges the data in the summary table below. Select **MAC** to display and arrange the data according to MAC address. Select **VID** to display and arrange the data according to VLAN group. Select **PORT** to display and arrange the data according to port number.
Transfer Type	Select **Dynamic to MAC forwarding** and click the **Transfer** button to change all dynamically learned MAC address entries in the summary table below into static entries. They also display in the **Static MAC Forwarding** screen. Select **Dynamic to MAC filtering** and click the **Transfer** button to change all dynamically learned MAC address entries in the summary table below into MAC filtering entries. These entries will then display only in the **Filtering** screen and the default filtering action is **Discard source**.
Cancel	Click **Cancel** to change the fields back to their last saved values.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port where the above MAC address is forwarded.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

40

ARP Table

40.1 Overview

This chapter introduces ARP Table.

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

40.1.1 What You Can Do

Use the **ARP Table** screen (Section 40.2 on page 299) to view IP-to-MAC address mapping(s).

40.1.2 What You Need to Know

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

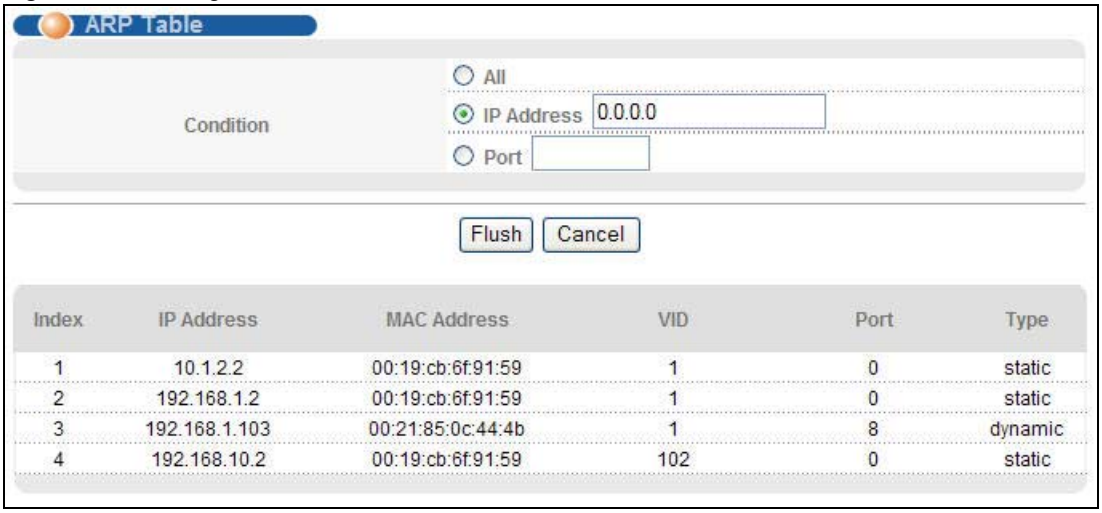
If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

40.2 Viewing the ARP Table

Use the ARP table to view IP-to-MAC address mapping(s) and remove specific dynamic ARP entries.

Click **Management** > **ARP Table** in the navigation panel to open the following screen.

Figure 199 Management > ARP Table



The following table describes the labels in this screen.

Table 126 Management > ARP Table

LABEL	DESCRIPTION
Condition	Specify how you want the Switch to remove ARP entries when you click **Flush**. Select **All** to remove all of the dynamic entries from the ARP table. Select **IP Address** and enter an IP address to remove the dynamic entries learned with the specified IP address. Select **Port** and enter a port number to remove the dynamic entries learned on the specified port.
Flush	Click **Flush** to remove the ARP entries according to the condition you specified.
Cancel	Click **Cancel** to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. **CPU** means this learned IP address is the Switch's management IP address.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

41

Configure Clone

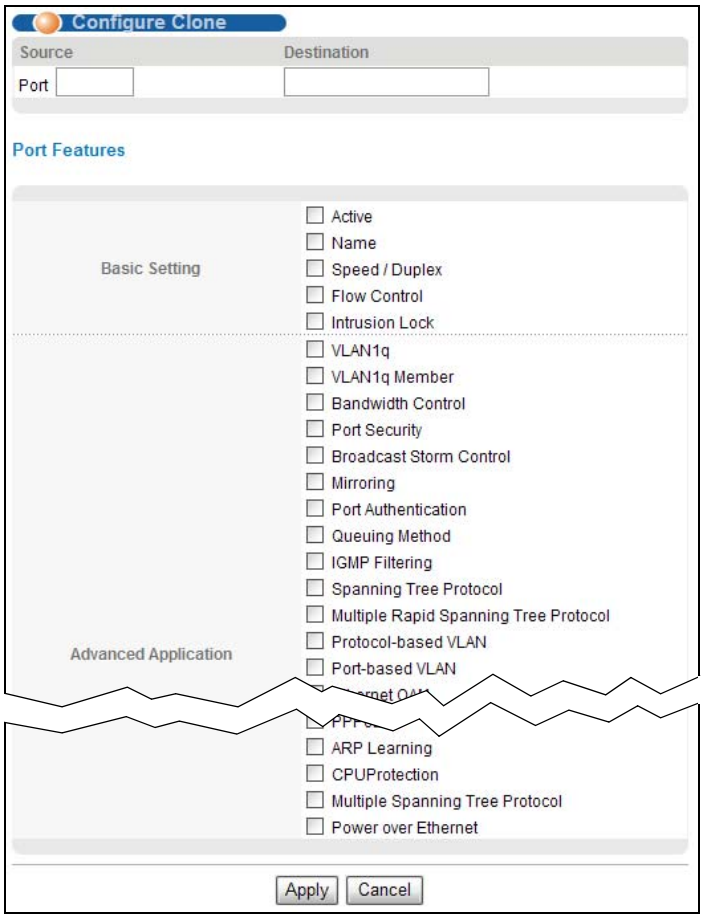
41.1 Overview

This chapter shows you how you can copy the settings of one port onto other ports.

41.2 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management** > **Configure Clone** to open the following screen.

Figure 200 Management > Configure Clone



The following table describes the labels in this screen.

Table 127 Management > Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port under the **Source** label. This port's attributes are copied. Enter the destination port or ports under the **Destination** label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: • **2, 4, 6** indicates that ports 2, 4 and 6 are the destination ports. • **2-6** indicates that ports 2 through 6 are the destination ports.
Basic Setting	Select which port settings (you configured in the **Basic Setting** menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (you configured in the **Advanced Application** menus) should be copied to the destination ports.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

42

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Switch Access and Login
- Switch Configuration

42.1 Power, Hardware Connections, and LEDs

The Switch does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the Switch.
2. Make sure the power adaptor or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the Switch.
4. If the problem continues, contact the vendor.

The **ALM** LED is on.

1. Disconnect and re-connect the power adaptor or cord to the Switch.
2. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 3.3 on page 36.
2. Check the hardware connections. See Section 42.1 on page 303.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adaptor or cord to the Switch.

5 If the problem continues, contact the vendor.

42.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default IP address is **192.168.1.1**.

2 Use the console port to log in to the Switch.

3 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 45.

I forgot the username and/or password.

1 The default username is **admin** and the default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 45.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.
- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Switch.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 3.3 on page 36.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)

5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See Section 4.6 on page 45.

6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the Switch.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.

Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.

3 Disconnect and re-connect the cord to the Switch.

4 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 45.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

I cannot see some of **Advanced Application** submenus at the bottom of the navigation panel.

The recommended screen resolution is 1024 by 768 pixels. Adjust the value in your computer and then you should see the rest of **Advanced Application** submenus at the bottom of the navigation panel.

There is unauthorized access to my Switch via telnet, HTTP and SSH.

Click the **Display** button in the **System Log** field in the **Management** > **Diagnostic** screen to check for unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **Management** > **Access Control** > **Remote Management** screen for telnet, HTTP and SSH (see Section 35.6 on page 268). Computers not belonging to the secured client set cannot get permission to access the Switch.

42.3 Switch Configuration

I lost my configuration settings after I restart the Switch.

Make sure you save your configuration into the Switch's nonvolatile memory each time you make changes. Click **Save** at the top right corner of the web configurator to save the configuration permanently. See also Section 34.5 on page 258 for more information about how to save your configuration.

43

Product Specifications

The following tables summarize the Switch's hardware and firmware features.

Table 128 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	Desktop design • GS2200-8 : 250*148*44.5 mm • GS2200-8HP: 330*230*44.5 mm 1U and standard 19" rack mountable • GS2200-24: 440*173*44 mm • GS2200-24P: 440*310*44 mm
Weight	GS2200-8: 1.34 Kg GS2200-8HP: 2.66 Kg GS2200-24 : 2.5 Kg GS2200-24P : 4.75 Kg
Power Specification	Power Rating : GS2200-8: 100-240VAC 50/60Hz 0.3A max. GS2200-8HP: 100-240VAC 50/60Hz 2.4A max. GS2200-24: 100-240VAC 50/60Hz 0.5A max. GS2200-24P: 100-240VAC 50/60Hz 2.5A max.
Power Consumption	GS2200-8: 12.3 Watt (max.) GS2200-8HP: 230 Watt (max.) GS2200-24 : 31 W (max.) GS2200-24P : 268 W (max.)

Table 128 Hardware Specifications

Interfaces	GS2200-8: 8 100/1000BASE-T GS2200-8HP: 8 100/1000BASE-T PoE GS2200-24: 24 100/1000BASE-T GS2200-24P: 24 100/1000BASE-T PoE 2 or 4 GbE Dual Personality interfaces (Each interface has one 1000Base-T RJ-45 port and one Small Form-Factor Pluggable (SFP) slot, with one port active at a time.) Note: The ports change to fiber mode directly when inserting the fiber module. Auto-negotiation Auto-MDIX One console port Compliant with IEEE 802.3/3u/3ab Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x)
LEDs	Per switch: PWR, SYS, ALM GS2200-8: Per GE Ethernet RJ-45 100/1000 port: LNK/ACT GS2200-24: Per GE Ethernet RJ-45 100/1000 port: LNK/ACT, FDX GS2200-24P/GS2200-8HP: Per GE PoE Ethernet RJ-45 100/1000 port: LNK/ACT, PoE Per mini-GBIC slot: LNK, ACT Per 1000BASE-T RJ-45 port (in dual personality interface): LNK/ACT, FDX (GS2200-24/24P only)
Operating Environment	Temperature: 0º C ~ 50º C (32º F ~ 122º F) Humidity: 10 ~ 95% (non-condensing)
Storage Environment	Temperature: -40º C ~ 70º C (-40º F ~ 158º F) Humidity: 10 ~ 95% (non-condensing)
Fuse Specification	250 VAC, T2A
Console port	D-Sub 9 pin Female (DCE)
Capacity	GS2200-8/8HP: 20 Gbps GS2200-24/24P: 56 Gbps
Forwarding Rate	GS2200-8/8HP: 14.9 million packets per second GS2200-24/24P: 41.7 million packets per second

Table 129 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234

Table 129 Firmware Specifications

FEATURE	DESCRIPTION
Number of Login Accounts Configurable on the Switch	4 management accounts configured on the Switch. Authentication via RADIUS and TACACS+ also available.
Maximum Frame Size	9 K (9216 bytes)
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address and VLAN group (ID).
DHCP (Dynamic Host Configuration Protocol) Relay	Use this feature to have the Switch forward DHCP requests to DHCP servers on your network.
IGMP Snooping	The Switch supports IGMP snooping, enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your Switch.
Differentiated Services (DiffServ)	With DiffServ, the Switch marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
Classifier and Policy	You can create a policy to define actions to be performed on a traffic flow grouped by a classifier according to specific criteria such as the IP address, port number or protocol type, etc.
Queuing	Queuing is used to help solve performance degradation when there is network congestion. The following scheduling services are supported: Strict Priority Queuing (SPQ) Weighted Round Robin (WRR), and Weighted Fair Queuing (WFQ). This allows the Switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.
Bandwidth Control	Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.
Broadcast Storm Control	Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.
Static Route	Static routes allow the Switch to communicate with management stations not reachable via the default gateway.
STP (Spanning Tree Protocol) / RSTP (Rapid STP)/MSTP (Multiple Spanning Tree Protocol)	(M)(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (M)(R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.
Loop Guard	Use the loop guard feature to protect against network loops on the edge of your network.
IP Source Guard	Use IP source guard to filter unauthorized DHCP and ARP packets in your network.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

Table 129 Firmware Specifications

FEATURE	DESCRIPTION
Port Authentication and Security	For security, the Switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch.
Authenticatio and Authorization	The Switch supports authentication and authorization services via RADIUS and TACACS+ AAA servers.
Device Management	Use the web configurator or commands to easily configure the rich range of features on the Switch.
Port Cloning	Use the port cloning feature to copy the settings you configure on one port to another port or ports.
Syslog	The Switch can generate syslog messages and send it to a syslog server.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or an FTP/TFTP tool to put it on the Switch. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the Switch's configuration and put it back on the Switch later if you decide you want to revert back to an earlier configuration.
Cluster Management	Cluster management (also known as iStacking) allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.
PPPoE IA	With the PPPoE Intermediate Agent enabled, the Switch can give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.
CPU Protection	You can limit the rate of protocol control packets (such as ARP, BPDU and/or IGMP) to be delivered to the CPU on a port.
Error Disable	You can set the Switch to take an action (such as to shut down a port or stop sending packets) on a port when the Switch detects a pre-configured error. You can also configure the Switch to automatically undo the action after the error is gone.
ARP Learning	You can configure the Switch to update the ARP table with with an ARP reply or a gratuitous ARP request and/or an APR request.

Table 130 Feature Specifications

L2 Bridging	16K MAC addresses (4-way associative hashed) Static MAC address filtering by source/destination Broadcast storm control in 1 second interval, 1 pps stepping Static MAC address forwarding (port lock)
Switching	Switching fabric: 20 Gbps or 56 Gbps, non-blocking Max. Frame size: 9 K bytes Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Prevent the forwarding of corrupted packets 148809 pps at 100 Mbps / 1488095 pps at 1 Gbps with 64 bytes packets

Table 130 Feature Specifications (continued)

STP	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Multiple Rapid Spanning Tree capability IEEE 802.1s Multiple Spanning Tree Protocol
QoS	IEEE 802.1p with 8 CoS per port 802.3x flow control SPQ,WFQ, or SPQ/WFQ combination capable Rule-based bandwidth control (ingress traffic metering/dropping 64Kb stepping) Rule-based traffic mirroring IGMP snooping (IGMP v1/v2/v3, 16 VLAN maximum - user configurable) DSCP to 802.1p priority mapping
VLAN	Port-based VLAN 802.1Q tag-based VLAN number of VLAN: 4K, 1000 static maximum GVRP for dynamic registration Private VLAN for port isolation Protocol-Based VLAN. IP subnet based VLAN
Link Aggregation	IEEE 802.3ad static and dynamic by LACP Eight groups (up to eight ports/group randomly selected)
Port mirroring	Rule-based port mirrorring Port-based mirroring Support port mirroring per IP/TCP/UDP
Bandwidth control	Supports rate limiting at 64 Kb increments
Broadcast Storm Control	Broadcast, Multicast, Unknown Uicast Storm Control 1 pps stepping
Rate Limiting	Support rate limiting per IP/TCP/UDP port
IP services	DHCP client DHCP relay
Filtering	Support L2 MAC filtering, L3 IP filtering, Layer 4 TCP/UDP socket
Multicast	IGMP snooping (IGMP v1/v2/v3, 16 VLAN maximum-user configurable)
AAA	Support RADIUS and TACACS+

Table 130 Feature Specifications (continued)

Security	Static MAC address filtering Static MAC address forwarding MAC Freeze IEEE 802.1x port-based authentication Limiting number of dynamic MAC addresses per port SSH v1/v2 SSL Multiple RADIUS servers Multiple TACACS+ servers 802.1X VLAN and bandwidth assignment. IP source guard Static IP/MAC binding DHCP snooping ARP Inspection ARP Freeze Guest VLAN PPPoE IA and option 82 Configurable ARP learning mode
PoE feature (GS2200-8HP and GS2200-24P only)	Classification mode Consumption mode
IPv6	DHCPv6: client and relay ICMPv6 IPv6 Path MTU NDP: host IPv6 address stateless auto-configuration: host

The following list, which is not exhaustive, illustrates the standards supported in the Switch.

Table 131 Standards Supported

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 894	Ethernet II Encapsulation
RFC 1112	IGMP v1
RFC 1155	SMI
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs

Table 131 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 1757	RMON
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2138	RADIUS (Remote Authentication Dial In User Service)
RFC 2233	ifVHCPacketGroup
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2674	P-BRIDGE-MIB, Q-BRIDGE-MIB
RFC 2865	RADIUS - Vendor Specific Attribute
RFC 2925	PING-MIB fand TRACEROUTE-MIB
RFC 3046	DHCP Relay
RFC 3164	Syslog
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP v3)
RFC 3580	RADIUS - Tunnel Protocol Attribute
IEEE 802.1ab	Link Layer Discovery Protocol (LLDP)
IEEE 802.1ag	Connectivity Fault Management (CFM)
IEEE 802.1x	Port Based Network Access Control
IEEE 802.1D	MAC Bridges
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1Q	Tagged VLAN
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1s	Multiple Spanning Tree Protocol (MSTP)
IEEE 802.3	Packet Format
IEEE 802.3ad	Link Aggregation
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet
IEEE 802.3at (GS2200-8HP only)	High Power over Ethernet
IEEE802.3az (GS2200-8 and GS2200-8HP only)	Energy Efficient Ethernet (EEE)
Safety	UL 60950-1 (GS2200-8/8HP only) CSA 60950-1 (GS2200-24/24P only) CNS 14336-1 (GS2200-8/8HP only) EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A) CNS 13438 (GS2200-8/8HP only)

A

Changing a Fuse

This appendix shows you how to remove and install fuses for the Switch.

If you use a fuse other than an included fuse, make sure it matches the fuse specifications in the chapter on product specifications.

Removing a Fuse

Disconnect all power from the Switch before you begin this procedure.

1. Remove the power cord from the Switch.
2. See the product specifications for the location of the fuse. Use a small flat-head screwdriver to carefully pry out the fuse housing.
3. A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing. Pull gently, but firmly, to remove the burnt out fuse from the fuse housing. Dispose of the burnt-out fuse properly.

Installing a Fuse

1. The Switch is shipped from the factory with one spare fuse included in a box-like section of the fuse housing. Push the middle part of the box-like section to access the spare fuse. Put another spare fuse in its place in order to always have one on hand.
2. Push the replacement fuse into the fuse housing until you hear a click.
3. Push the fuse housing back into the Switch until you hear a click.
4. Plug the power cord back into the unit.

B

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 132 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

Table 132 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 132 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

C

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者

這是甲類的資訊產品，在居住的環境使用時，

可能造成射頻干擾，在這種情況下，

使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

Numbers

802.1P priority 76

A

AAA 182
AAA (Authentication and Authorization) 182
access control
  limitations 261
  login account 266
  remote management 268
  service port 268
  SNMP 270
address learning, MAC 92, 94
Address Resolution Protocol (ARP) 250, 299, 301, 302
administrator password 267
age 121
aggregator ID 140, 142
airflow 36
applications
  backbone 23
  bridging 24
  IEEE 802.1Q VLAN 25
  switched workgroup 24
ARP
  how it works 250, 299
  viewing 299
ARP (Address Resolution Protocol) 250, 299
ARP inspection 194, 213
  and MAC filter 213
  configuring 214
  syslog messages 214
  trusted ports 214
authentication 182
  setup 188
Authentication and Authorization, see AAA 182
authorization 182
  privilege levels 188, 190
  setup 188
auto-crossover 34
automatic VLAN registration 84

B

back up, configuration file 258
bandwidth control 129
  egress rate 130
  ingress rate 130
  setup 130
basic settings 66
basic setup tutorial 51
binding 193
binding table 193
  building 194
BPDUs (Bridge Protocol Data Units) 110
Bridge Protocol Data Units (BPDUs) 110
broadcast storm control 132

C

CDP 222
certifications 321
  notices 321
  viewing 321
CFI (Canonical Format Indicator) 83
changing the password 44
Cisco Discovery Protocol, see CDP
CIST 127
Class of Service (CoS) 240
classifier 154, 156
  and QoS 154
  editing 156
  example 158
  overview 154
  setup 154, 156
  viewing 156

cloning a port See port cloning
cluster management 290
and switch passwords 293
cluster manager 290, 293
cluster member 290, 293
cluster member firmware upgrade 295
network example 290
setup 292
specification 290
status 291
switch models 290
VID 293
web configurator 294
cluster manager 290
cluster member 290
Common and Internal Spanning Tree, See CIST 127
configuration 239
change running config 257
configuration file 45
backup 258
restore 45, 258
saving 256
configuration, saving 44
console port 33
copying port settings, See port cloning
copyright 321
CPU management port 96
CPU protection
configuration 232
overview 231
current date 70
current time 69

D

daylight saving time 70
default Ethernet settings 34
DHCP 244
configuration options 244
modes 244
Option 82 245
overview 244
relay agent 244
relay agent information 245
relay example 248
setup 247
VLAN setting 247
DHCP relay 245
configuration 246
example 247
DHCP relay option 82 212
DHCP snooping 51, 194, 211
configuring 213
DHCP relay option 82 212
trusted ports 211
untrusted ports 211
DHCP snooping database 212
diagnostics 285
Ethernet port test 286
ping 286
system log 285
Differentiated Service (DiffServ) 240
DiffServ 240
activate 241
DS field 240
DSCP 240
network example 241
PHB 241
dimensions 307
disclaimer 321
DS (Differentiated Services) 240
DSCP
service level 240
what it does 241
DSCP (DiffServ Code Point) 240
Dynamic Host Configuration Protocol, see DHCP
dynamic link aggregation 137

E

egress port 99
egress rate, and bandwidth control 130
error disable detect 233
error disable recovery
configuration 234
overview 231
Ethernet broadcast address 250, 299
Ethernet port test 286
external authentication server 183

F

fan speed 68
FCC interference statement 321
file transfer using FTP
  command example 259
filename convention, configuration
  configuration
    file names 259
filtering 107
  rules 107
filtering database, MAC table 296
firmware 67
  upgrade 257, 295
flow control 76
  back pressure 76
  IEEE802.3x 76
forwarding
  delay 121
frames
  tagged 91
  untagged 91
front panel 31
FTP 259
  file transfer procedure 259
  restrictions over WAN 260
fuse 315
  replacement 315

G

GARP 84
GARP (Generic Attribute Registration Protocol) 84
GARP terminology 84
GARP timer 71, 84
general features 310
general setup 69
getting help 46
Gigabit ports 33
GMT (Greenwich Mean Time) 70
GVRP 84, 90, 91
  and port assignment 91
GVRP (GARP VLAN Registration Protocol) 84

H

hardware installation 27
hardware monitor 67
hardware overview 31
hello time 121
hops 121
HTTPS 278
  certificates 278
  implementation 278
  public keys, private keys 278
HTTPS example 279
humidity 308

I

IEEE 802.1p, priority 72
IEEE 802.1x
  activate 147, 186
  port authentication 145
  reauthentication 148
IGMP
  version 168
IGMP (Internet Group Management Protocol) 168
IGMP filtering
  profile 175
  profiles 172
IGMP leave timeout
  fast 172
  mormal 172
IGMP snooping 168
  and VLANs 169
  MVR 169
  setup 174
IGMP throttling 173
ingress port 99
ingress rate, and bandwidth control 130
install
  fuse 315
installation
  desktop 27
  precautions 27
  rack-mounting 27
  transceivers 34
installation scenarios 27

IP address 74
IP interface 73
IP setup 72
IP source guard 193, 194
  ARP inspection 194, 213
  DHCP snooping 194, 211
  static bindings 194
IP subnet mask 74

L

L2PT 219
  access port 220
  CDP 219
  configuration 221
  encapsulation 219
  LACP 220
  MAC address 219
  mode 220
  overview 219
  PAgP 220
  point to point 220
  STP 219
  tunnel port 220
  UDLD 220
  VTP 219
LACP 137, 222
  system priority 143
  timeout 143
Layer 2 protocol tunneling, see L2PT
LEDs 36
limit MAC address learning 153
link aggregation 137
  dynamic 137
  ID information 138
  setup 140, 142
  status 139
  traffic distribution algorithm 139
  traffic distribution type 141
  trunk group 137
Link Aggregation Control Protocol (LACP) 137
Link Aggregation Control Protocol, see LACP 137
lockout 44
log 285
login 39
  password 44
login account
  Administrator 266
  non-administrator 267
login accounts 266
  configuring via web configurator 266
  multiple 266
  number of 266
login password 267
loop guard 215
  examples 216
  port shut down 217
  setup 217
  vs. STP 215

M

MAC (Media Access Control) 67
MAC address 67, 250, 299
  maximum number per port 153
MAC address learning 92, 94, 101, 153
  specify limit 153
MAC filter
  and ARP inspection 213
MAC freeze 152
MAC table 296
  display criteria 298
  how it works 296
  sorting criteria 298
  transfer type 298
  viewing 297
maintanence
  configuration backup 258
  firmware 257
  restoring configuration 258
maintenance 255
  current configuration 255
  main screen 255
Management Information Base (MIB) 270
management port 99
managing the device
  good habits 26
  using FTP. See FTP. 26
  using Telnet. See command interface. 26
  using the command interface. See command interface. 26
man-in-the-middle attacks 213

max
age 121
hops 121
MDIX (Media Dependent Interface Crossover) 34
MIB
and SNMP 270
supported MIBs 271
MIB (Management Information Base) 270
mirroring ports 134
monitor port 135
mounting brackets 28
MRSTP status 118
MST ID 127
MST Instance, See MSTI 127
MST region 126
MSTI 127
MSTP 109, 112
bridge ID 124, 125
configuration 120, 123
configuration digest 125
forwarding delay 121
Hello Time 124
hello time 121
Max Age 124
max age 121
max hops 121
path cost 122
port priority 122
revision level 121
status 123
MTU (Multi-Tenant Unit) 70
Multicast 168
multicast 168
802.1 priority 172
and IGMP 168
IGMP throttling 173
IP addresses 168
overview 168
setup 171, 172
multicast group 175
multicast VLAN 178
Multiple Rapid Spanning Tree Protocol 111
Multiple RSTP 111
Multiple Spanning Tree Protocol, See MSTP 109, 112
Multiple STP 112
MVR 169
configuration 176
group configuration 178
network example 169
MVR (Multicast VLAN Registration) 169

N

network applications 23
network management system (NMS) 270
NTP (RFC-1305) 69

P

PAGP 222
password 44
administrator 267
PHB (Per-Hop Behavior) 241
ping, test connection 286
policy 161
and classifier 161
and DiffServ 160
configuration 161
example 164
overview 160
rules 160
viewing 163
Port Aggregation Protocol, see PAgP
port authentication 145
and RADIUS 183
IEEE802.1x 147, 186
port based VLAN type 71
port cloning 301, 302
advanced settings 301, 302
basic settings 301, 302
port details 63
port isolation 99
port mirroring 134, 135
direction 135
egress 135
ingress 135
port redundancy 137
port security 151
limit MAC address learning 153

MAC address learning 151
overview 151
setup 152, 217, 221
port setup 75
port status 61
port VLAN ID, see PVID 91
port VLAN trunking 85
port-based VLAN 96
all connected 99
port isolation 99
settings wizard 99
ports
diagnostics 286
mirroring 134
speed/duplex 76
standby 138
power
voltage 68
power connector 35
power consumption 307
power specification 307
power status 68
PPPoE IA
trusted ports 225
untrusted ports 225
priority level 72
priority, queue assignment 72
product registration 322
protocol based VLAN 94
and IEEE 802.1Q tagging 94
application example 94
configuration example 99
isolate traffic 94
priority 95
un-tagged packets 95
PVID 84
PVID (Priority Frame) 84

Q

QoS
and classifier 154
queue weight 166
queuing 165
SPQ 165
WRR 165
queuing method 165, 167

R

rack-mounting 27
RADIUS 182, 183
advantages 183
and port authentication 183
and tunnel protocol attribute 191
Network example 182
server 183
settings 183
setup 183
Rapid Spanning Tree Protocol, See RSTP. 109
rear panel connections 35
reboot
load configuration 257
reboot system 257
registration
product 322
related documentation 3
remote management 268
service 269
trusted computers 269
removing fuses 315
resetting 45, 256
to factory default settings 256
restoring configuration 45, 258
RFC 3164 287
Round Robin Scheduling 165
RSTP 109

S

safety certifications 313
safety warnings 8
save configuration 44, 256
Secure Shell See SSH
service access control 268
service port 268
Simple Network Management Protocol, see SNMP
Small Form-factor Pluggable (SFP) 34

SNMP 270
agent 270
and MIB 270
and security 271
authentication 265, 266
communities 263
management model 270
manager 270
MIB 271
network components 270
object variables 270
protocol operations 270
security 265, 266
setup 262
trap group 264
users 265
version 3 271
versions supported 270
SNMP traps 271, 272, 274, 276
setup 264
Spanning Tree Protocol, See STP. 109
SPQ (Strict Priority Queuing) 165
SSH
encryption methods 278
how it works 277
implementation 278
SSH (Secure Shell) 277
SSL (Secure Socket Layer) 278
standby ports 138
static bindings 194
static link aggregation example 143
static MAC address 101
static MAC forwarding 92, 94, 101
static multicast address 103
static multicast forwarding 103
static routes 239
static trunking example 143
Static VLAN 88
static VLAN
control 89
tagging 89
status 40, 61
link aggregation 139
MSTP 123
port 61
port details 63
power 68
STP 115, 118
VLAN 86
STP 109, 222
bridge ID 116, 119
bridge priority 114, 117
configuration 114, 117
designated bridge 110
forwarding delay 115, 118
Hello BPDU 110
Hello Time 115, 116, 118, 119
how it works 110
Max Age 115, 116, 118, 119
path cost 110, 115, 118
port priority 115, 118
port state 111
root port 110
status 115, 118
terminology 110
vs. loop guard 215
subnet based VLAN 93
and DHCP VLAN 93
priority 93
setup 92
subnet based VLANs 91
switch lockout 44
switch reset 45
switch setup 71
syntax conventions 6
syslog 214, 287
protocol 287
server setup 289
settings 287
setup 287
severity levels 287
system information 67
system log 285
system reboot 257

T

TACACS+ 182, 183
setup 186
TACACS+ (Terminal Access Controller Access-Control System Plus) 182
tagged VLAN 83
temperature 308

temperature indicator 67
terminal emulation 33
time
  current 69
  time zone 70
Time (RFC-868) 69
time server 69
time service protocol 69
  format 69
trademarks 321
transceiver MultiSource Agreement (MSA) 34
transceivers 34
  installation 34
  removal 35
traps
  destination 263
trunk group 137
trunking 137
  example 143
trusted ports
  ARP inspection 214
  DHCP snooping 211
  PPPoE IA 225
tunnel protocol attribute, and RADIUS 191
tutorials 51
  DHCP snooping 51
Type of Service (ToS) 240

U

UDLD 222
UniDirectional Link Detection, see UDLD
untrusted ports
  ARP inspection 214
  DHCP snooping 211
  PPPoE IA 225
user profiles 183

V

Vendor Specific Attribute, See VSA 190
ventilation 27
VID 86, 87
  number of possible VIDs 84
  priority frame 83
VID (VLAN Identifier) 83
VLAN 70
  acceptable frame type 91
  automatic registration 84
  ID 83
  IGMP snooping 169
  ingress filtering 90
  introduction 70, 83
  number of VLANs 86
  port number 87
  port settings 90
  port-based VLAN 96
  port-based, all connected 99
  port-based, isolation 99
  port-based, wizard 99
  PVID 91
  static VLAN 88
  status 86, 87
  subnet based 91
  tagged 83
  trunking 85, 91
  type 71, 85
VLAN (Virtual Local Area Network) 70
VLAN ID 74
VLAN Trunking Protocol, see VTP
VLAN, protocol based, See protocol based VLAN 94
VSA 190
VT100 33
VTP 222

W

wall mounting 29
warranty 322
  note 322
web configurator 39
  getting help 46
  home 40
  login 39
  logout 46
  navigation panel 41
weight, queuing 166
Weighted Round Robin Scheduling (WRR) 166
WRR (Weighted Round Robin Scheduling) 165

Z

ZyNOS (ZyXEL Network Operating System) 259